RAND CORPORATION

CHILDREN AND FAMILIES
EDUCATION AND THE ARTS
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INFRASTRUCTURE AND TRANSPORTATION
INTERNATIONAL AFFAIRS
LAW AND BUSINESS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
TERRORISM AND HOMELAND SECURITY

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis.

This electronic document was made available from www.rand.org as a public service of the RAND Corporation.

Skip all front matter: Jump to Page 1

## Support RAND

Purchase this document

Browse Reports & Bookstore

Make a charitable contribution

## For More Information

Visit RAND at www.rand.org

Explore the RAND Corporation

View document details

### Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND electronic documents to a non-RAND website is prohibited. RAND electronic documents are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see RAND Permissions.

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **2014** | | **00-00-2014 to 00-00-2014** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **How Do We Know What Information Sharing Is Really Worth? Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **RAND Corporation,National Defense Research Institute,1776 Main Street, P.O. Box 2138,Santa Monica ,CA,90407-2138** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **Same as Report (SAR)** | **33** | |

This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.

RAND CORPORATION

# How Do We Know What Information Sharing Is Really Worth?

## Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts

*Brian A. Jackson*

### Key findings

- The lack of literature on evaluating information sharing, coupled with passionate arguments both for and against the value of such efforts, has produced a stunted policy debate that is insufficient to support reasoned and reasonable tradeoffs among these programs and other ways to pursue the goals they are designed to advance.
- With a clearer framing of the evaluable goals sharing programs are pursuing, data on organizational outcomes can be linked to different ways of assessing the "dosage" of exposure to information sharing at different levels.
- New analytic techniques that enable matching of individual users and comparison of outcomes at a very disaggregated level appear particularly promising for assessing existing initiatives.
- Systematic approaches like "but-for" analyses and structures that tie sharing to the outcomes it is designed to achieve provide paths toward improved measurement of the value of information sharing and fusion efforts.

**SUMMARY** ■ Information sharing between security, intelligence, and law enforcement organizations has become a central focus of U.S. domestic security efforts. The value of being able to better "connect the dots" to detect threats is obvious, and the identification of failures to do so after incidents occur is routine. The importance of information sharing also reaches beyond counterterrorism and domestic security, with multiagency and multijurisdictional data systems playing central roles in fighting crime more broadly. Yet, in spite of the intense focus on information sharing, the ability to fairly and accurately measure the value of these—sometimes expensive—efforts remains limited. Anecdotes of success and failure can be found on both sides, resulting in a policy debate that has been insufficiently productive to effectively weigh investments in this area.

The analysis presented here attempts to help address that shortfall by exploring methodologies to enable better evaluation of information sharing and fusion activities. The framing of the analysis is intentionally broad, covering not only high-profile terrorism information sharing efforts, like the Department of Homeland Security's fusion center program, but also systems used every day by police departments to share records and biometric data to apprehend criminal suspects. The report discusses the evaluation concerns for such systems, reviews the literature that has sought to evaluate them, and frames a path forward for future evaluation efforts.

## INTRODUCTION

In the years since the terrorist attacks of September 11, 2001, information sharing and fusion efforts have been a central part of both domestic security and attempts to improve national-level military and intelligence performance. This focus can be traced back to the report of the 9/11 Commission, which included improvements in information sharing—and the integration of efforts across security and intelligence agencies—among its recommendations (9/11 Commission, 2004, pp. 416–419). Those recommendations catalyzed significant efforts and expenditures, which, appropriately, has raised questions about how to assess what that investment has returned. As resource constraints place increasing pressure on government and security efforts, measuring the effectiveness of those efforts becomes increasingly important so that reasonable tradeoffs can be made. Past assessment methods have not been up to that task, however, necessitating both a reevaluation of what we know about the effectiveness of information sharing and the development of better ways to measure it going forward.

### A Decade—and More—of Information Sharing Efforts

A focus on improved information sharing as a key element of domestic security has persisted in the years since 9/11, and its policy prominence is reflected in the fact that there are now two national strategies that address the issue: (1) the *National Strategy for Information Sharing* released in October 2007 and (2) the *National Strategy for Information Sharing and Safeguarding* released in December 2012, which explicitly states that it complements rather than replaces the earlier document. Reflecting the shared responsibility among widely varied organizations and agencies, concerns about information sharing in domestic security relate not only—perhaps not even centrally—to sharing among different federal-level agencies but also to sharing between different levels of government (federal, state, local, and tribal) and between government and non-government or private entities.

The requirement to wage effective counterinsurgency warfare in both Iraq and Afghanistan similarly focused attention on information sharing and the fusion of intelligence from many sources to make it possible to battle the insurgent and terrorist organizations that were central adversaries in both conflicts (see Lamb and Munsing, 2011, for a review). Activities in those conflicts led to a variety of efforts to promote sharing among intelligence and military organizations and, with members of the interagency involved, linking the resulting shared picture of the conflict to effective operations.

Though information sharing became prominent on the national scene after the 9/11 terrorist attacks, a variety of systems and activities to share security-related information among federal agencies; state, local, and tribal law enforcement; and other organizations existed well before that time. Some terrorism-focused information sharing efforts, such as the FBI's Joint Terrorism Task Forces (JTTFs), were in operation many years before 9/11 (9/11 Commission, 2004, pp. 81–82). Systems for sharing criminal-justice data to combat crime have also existed for a long time—in some cases, decades. National-level criminal-justice information sharing includes government efforts such as the resources maintained by the Criminal Justice Information Services (CJIS) section of the FBI and the Law Enforcement Online (LEO) system. The Regional Information Sharing System (RISS) links criminal-justice organizations in all fifty states through six regional sharing centers and has been in existence for more than 30 years. High Intensity Drug Trafficking Area multijurisdictional task forces (among other efforts to address violent crime and drug-related activities) were established starting in 1990 to synchronize drug-enforcement activities across agencies, including fostering—even forcing—interagency information sharing (see Russell-Einhorn, Ward, and Seeherman, 2004). Recent efforts to expand these information sharing infrastructures (e.g., the development of the FBI's N-DEx system), while occurring in an environment where concern about terrorism is prominent, are also focused on improving broader criminal-justice performance (ISE, undated; Sandler, 2010). Finally, extensive standards efforts, including the Global Justice Information Sharing Initiative (GLOBAL) and the National Information Exchange Model (NIEM), are aimed at making law enforcement information systems more interoperable and therefore facilitating the sharing of information among them.

The post–9/11 focus on information sharing catalyzed many changes in agency activities and behaviors and the creation of new programs and systems to improve national capabilities to battle terrorism and address the challenges inherent in modern counterinsurgent warfare. At the federal level, a significant initiative focused on the sharing of terrorism-related information—the Information Sharing Environment (ISE)—was implemented, along with a variety of other information technology-based efforts to improve links among different organizational entities. Interagency and multiagency

task forces were created (e.g., the DHS fusion center program), and existing cross-organizational teams like the JTTFs were expanded or augmented. Organizations like the Information Sharing and Analysis Centers (ISACs) were designed to bridge government and private sector entities. A 2006 survey by the Justice Research and Statistics Association identified more than 100 information sharing systems, from the national level down to the local level, focused on law enforcement alone (Wagner, 2006).[1]

Existing agencies made significant changes in their behavior, shifting from processes and organizational habits that held information close to greater willingness to share "their" data with others. For example, the FBI described its post-9/11 changes in practice as follows:

> Also of great necessity is the ability to share real-time information that allows both the FBI and its partners the world over to cross jurisdictional boundaries and quickly "connect the dots" when every minute counts. Gone are the days when information was held onto for fears of compromising investigations; the benefits of full and open sharing with our partners has proven time and time again to be more valuable than the close holding of intelligence. (McFeely, 2011)

A central motivator was the perception that the compartmentalization of information for security purposes—e.g., national-security classification of data with access control based on individuals' or organizations' "need to know"—and bureaucratic behaviors that incentivized the hoarding of data for use by the originating organization were central barriers to effective national and domestic security. Participation in such efforts at different levels of government spread and deepened, with available survey data indicating broad uptake at different levels of government. The ISE 2012 Annual Report to Congress indicated that 79 percent and 68 percent of federal agencies surveyed reported participation in JTTFs and fusion centers, respectively (ISE, 2012, p. A-4). An earlier survey of police department participation in information sharing systems (Wagner, 2005) showed extensive participation in at least some interagency information sharing efforts:[2] "While most chiefs responding to this survey reported involvement with multiagency information sharing, agencies serving populations over 100,000 are much more likely to be involved than those agencies serving smaller populations." Overall participation was approximately 80 percent for the largest departments and slightly higher for departments serving populations of between 100,000 and 250,000; it fell to just over 60 percent for departments protecting 25,000 and 50,000 people. Respondents to the survey were also generally satisfied with the results of information sharing: "Agencies currently involved in data sharing efforts find them valuable; between 65% and 75% of all groups of respondents reported that the effort was very valuable" (Wagner, 2005, pp. 17–18).

## Policy Debate on Information Sharing: Strong Views, Weaker Data

Reflecting the interest in information sharing as a component of domestic security since 9/11, the policy literature is replete with analyses that argue the need for "more" information sharing (over an undefined current baseline) and analyses arguing that existing efforts are not working to achieve their goal of shared data.[3] The proliferation of efforts by different agencies has led to questions from oversight authorities about potential duplication of systems and whether federal funds for information sharing are being utilized efficiently (e.g., GAO, 2013a, b; Permanent Subcommittee on Investigations, 2012, p. 43; Powner, 2007). Questions have also been raised about the value of key information sharing programs, notably in the 2012 Senate staff report focusing on the Department of Homeland Security (DHS) fusion centers' role in counterterrorism that concluded that the federal government, and DHS in particular, has "little to show" for the resources invested in these programs (Permanent Select Committee on Investigations, 2012, p. 9). Concerns about the value of information sharing efforts are not new and are not limited to fusion centers; questions have been asked for many years about the amount, relevance, and value of the information that is flowing—particularly from the federal government to other agencies (Davies and

The proliferation of efforts by different agencies has led to questions about potential duplication of systems and whether federal funds for information sharing are being utilized efficiently.

Plotkin, 2005, p. 62). The effect of information sharing activities on personal privacy and civil liberties has also been raised, since the potential for information collected in one location to be broadly shared could be perceived as increasing government intrusion into the lives and activities of citizens.[4]

Balanced against the concerns raised by these efforts is an enduring belief, supported by examples of these programs contributing to counterterrorism and law enforcement success, of the value of information sharing efforts.[5] Though anecdotes of success, even in multiples, are not enough in themselves to substantiate the value of multimillion dollar programs, they do show how bridging the divide between separate intelligence, law enforcement, military, and domestic security agencies can produce real benefits.

The often diametrically opposed viewpoints about the value of information sharing programs have resulted to date in a somewhat stunted policy debate, without clear data and grounds to unambiguously make the case for or against individual sharing or fusion efforts' value. Some evaluation efforts (discussed below) have been made, but they have not resolved the stark disagreement on the value of these programs. Rigorous and defensible approaches to measure the benefits of information sharing efforts are needed to enable comparison with the costs associated with creating and pursuing those efforts. Recognition of the need for such measures is not new; for example, the need to "develop ways to measure the success of criminal intelligence sharing and recognize those individuals involved in that success" was one of eight recommendations presented at a 2007 summit on post-9/11 intelligence sponsored by the Department of Justice, the PM-ISE, DHS, and the International Association of Chiefs of Police (IACP, 2008, p. 4).

Although the primary focus of this discussion is on assessing the benefits of information sharing, better measures of the costs of these efforts are needed as well. Some costs are straightforward to assess (e.g., the procurement cost of an information system), but others are more difficult. For example, a sharing effort will likely require the direct efforts of many people (in management, operations, and oversight), but that investment may be offset by time savings for other personnel who use the system, making the net personnel cost less than it might appear. Although it is clear that the expansion of information sharing efforts in recent years has increased the amount of money spent on such programs, the full extent of those expenditures is not clear.[6] The intangible costs of information sharing efforts on personal privacy are similarly difficult to assess and compare with the potential benefits (Lester, 2009; Jackson, 2009b). Better evaluation is therefore needed on "both sides of the ledger," both to fully understand and to justify the amounts of money spent on such programs.

### Reevaluating What We Know, Exploring Paths Forward

Through an in-depth review and synthesis of the literature on information sharing efforts, this exploratory analysis addresses the following questions:

- What are information sharing and fusion efforts designed to achieve?
- How have information sharing efforts been evaluated to date?
- Are there better ways of evaluating information sharing and fusion efforts?

As with all evaluation efforts, the foundation of the present analysis is the simple premise that the value of programs cannot be reasonably and fairly assessed without a clear understanding of the goal—or, more frequently, the multiple goals—they are designed to achieve. Examination of those goals should take advantage of evaluation efforts that have been done previously, but past evaluations have not provided enough insight to enable a robust debate on this issue. The first two questions therefore lead to the third, which is the key policy analysis and evaluation problem for an era in which information sharing technologies and activities are becoming increasingly pervasive and important.

Effective evaluation is needed to assess information sharing and fusion efforts in order to judge whether the benefit they produce outweighs their associated costs. More importantly, it is a necessary step toward answering the much broader question of how those efforts compare with other approaches to achieve the same security ends. In an era of resource constraints, only that broader understanding will make it possible to balance investments in these programs with other policy options designed to achieve the same ends, in an effort to get the most security at the least cost to the public purse.

## WHAT ARE INFORMATION SHARING AND FUSION EFFORTS DESIGNED TO ACHIEVE?

Asking what information sharing activities are supposed to do seems, at least on its face, a simple question. Clearly, they are intended to share information. And they are supposed to do so to produce better security.[7] After events that are viewed

as intelligence and security failures, a common explanation is that the "dots"—individual pieces of information related to a threat or criminal—were not "connected," either because their significance was not understood or because they were never "assembled" (i.e., even if they were known, they were known by different people or organizations and as a result were not available to be analyzed together).

Although these explanations do not take into account the benefit that hindsight provides in determining which of many pieces of information are important and salient, information sharing is often perceived as the solution to this problem. By bringing data together in one place, it is more likely that individuals with the potential to understand it will see it and—by extension—less likely that signals of impending harm or insights that could break criminal cases will be missed. The recurring nature of this perception in domestic security policy was emphasized by the fact that discussions after the Boston Marathon bombing in 2013 were strikingly similar to those that occurred immediately after the 9/11 attacks.

Examination of the policy debate surrounding information sharing and the details of existing information sharing programs, however, reveals a more complicated picture. In public discussions, the term *information sharing* is often used to describe very different systems and activities that are actually seeking to achieve somewhat different things. Although many activities can be usefully placed into this general category, the lack of clarity would appear to be one driver of the often muddled and imprecise policy debate. Similarly, because of the ways such different systems function and the different goals they are trying to achieve, a simple answer that "more sharing" is the solution to perceived security shortfalls does not hold up to examination.

To drill down into the issues and get to a more nuanced understanding of the effects of these efforts, we must first more clearly define the different modes and goals that are often included under the general rubric of information sharing. To do so, this study draws on the full range of literature and examples from intelligence, criminal justice, and other information sharing activities to examine different modes of sharing, the types of information being shared, and the linkage between sharing and the outcomes it is designed to achieve.

## Many Pipelines for Sharing Information

An individual or organization can become aware of information and analyze or act on it either if it collects the information itself or if there is a "pipeline" connecting it to another person or agency that already possesses it (see Libicki and Pfleeger, 2004, for a review). In practical terms, the nature of such linkage and how well a link performs can vary considerably:

- *The linkage can be technology-based or can exist as connections between people who work in an organization.* Information sharing is often thought of as being technology driven, and there is a wide variety of technology systems whose goal is to move data from one organization to another: computer networks, shared workspaces, listservs, data warehouses, federated datasets, and so on. However, social networks that exist among people are also effective—sometimes even more effective—conduits for sharing.[8] Discussions of federal interagency functioning often cite the importance of members of one agency calling trusted colleagues at another agency to convey intelligence or other information they believe they need to know (e.g., see Hawley and Means, 2012). The value of direct human-to-human information sharing is a central rationale for entities such as joint task forces or fusion centers that put members of different organizations in the same place to interact and work together on a daily basis. Organizations also exchange staff to intentionally build such links.
- *Linkages vary in the extent to which they automatically "push" information to other agencies or enable agencies to "pull" information from others.* A central difference between information sharing efforts and systems is whether they automatically send data out to other organizations or share only by request. Systems that link the data of one agency to another may push essentially everything outward; broadcast-type intelligence sharing (e.g., an analytic organization publishing the results of its work) also falls into the push category. Other database systems are query-based (e.g., a query entered into the system seeking information about an individual, incident, or other variable of interest "pulls" relevant information).
- *Linkages vary in whether they directly connect organizations or have connections mediated through another entity.* Some information technology (IT) systems directly connect two organizations for information sharing purposes (e.g., shared dispatch systems among response organizations in adjacent jurisdictions), while other entities can serve as bridges between organizations. Multiagency entities like fusion centers or task forces can serve bridging roles, as can some nongovernmental organizations, common data warehouses, and federal organizations that link entities inside and outside government.

- *Linkages vary in the amount of "filtering" they perform on the information passed.* Information sharing links vary in the extent to which they restrict the data that go out to others. Since security, intelligence, and law enforcement information can be sensitive for a variety of reasons, wholly unrestricted sharing would be expected to be comparatively uncommon. Issues of security (e.g., protection of the identity of confidential sources) or sensitivity (e.g., data relating to internal investigations) necessitate limits on transparency. Categories or compartments within information classification systems act as filters that are designed to limit how information travels, either in technical systems or between individuals. To strike a balance, some IT systems (e.g., N-DEx) make it possible to share the fact that there is a relevant record in an organization but require direct person-to-person contact before more data are shared. Though these and other types of "filters" might seem counter to the intent of such systems, filtering is not necessarily negative given the real potential for creating information overload from "oversharing" of data, which could itself undermine the value of the efforts.[9]

Figure 1 presents some of the variations that exist in information sharing, in both technological and human-mediated information sharing processes. In all cases shown in the figure, information sharing can be full or partial (e.g., filters may be present in the linkages) and may range from real-time, constant sharing to episodic interaction between agencies. Modes of sharing vary from the highly technical (e.g., integrating data systems across organizations, shown at the far left of Figure 1) to entirely human-based modes (e.g., informal interactions among colleagues, shown at the far right.) The amount of organizational and technological structure around sharing falls along a spectrum and can involve separate "mediating" entities between the sharing organizations. Human-based mediators include multiagency organizations like the fusion centers or JTTFs, while technological versions include data warehouses that combine multiagency data in one place for common use.

In current intelligence, law enforcement, and other governmental communities, examples of information sharing activities in all of these categories are readily available. Lists of acronyms, names of secure and public systems, and organizations dedicated to moving information ranging from individual data points (e.g., license plate numbers from crime scenes) to polished analytic products (e.g., finished intelligence published in classified data portals) to very tactical warnings and direction (e.g., threat advisories of suspected terrorist attacks) could—and have—filled pages (e.g., Wagner, 2006; Carter, 2004; Jackson, Noricks, and Goldsmith, 2009).

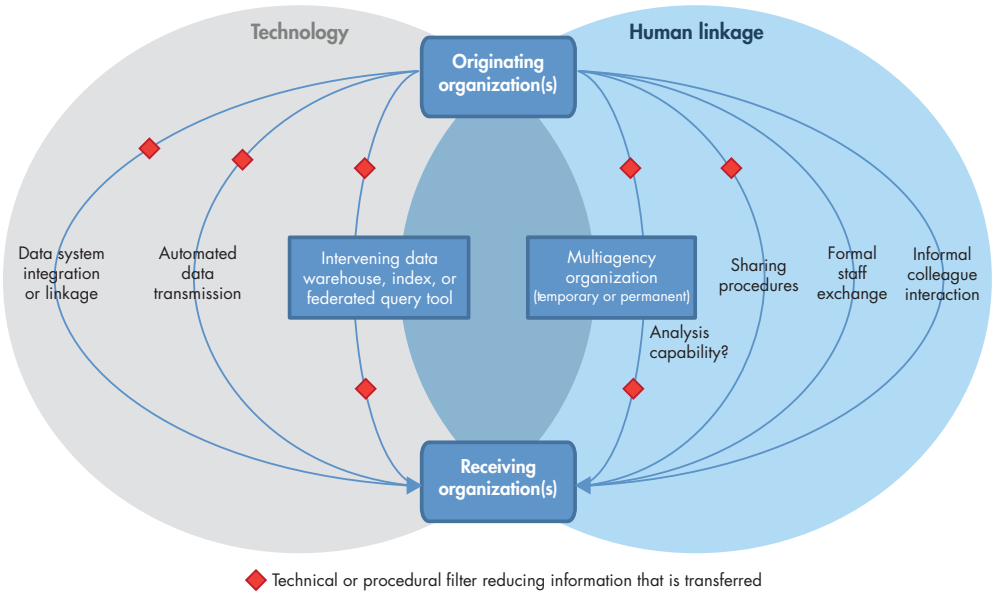
Even within classes, however, there is considerable variation in the ways information sharing is actually accomplished. Fusion centers may be the most publicly recognizable example of a multiagency organization charged with sharing information. What constitutes a fusion center varies, however. Some are implemented as physical locations where members of different agencies collaborate face to face, while others are shared technological workspaces where collaborative work occurs virtually (Davis et al., 2010, pp. 47–57). Because of this variation, efforts to measure information sharing must be compatible with a range of models and characteristics of existing efforts to appropriately represent the diversity that can exist even within generally similar systems or efforts.

## Sharing What Information, and Why?

With the impetus for broader information sharing among different levels of government and varied communities coming from 9/11 and the threat of terrorism, the most frequently cited goal is detecting future terrorist plots—where sharing fixes the problem of the data that might provide a picture of a plot being resident in different organizations. However, the term *information sharing* is also used to describe activities that are distinct from the intuitive and easy-to-understand concept of collecting all the dots into one place so they can be analyzed and understood. This broader definition is a feature of the policy literature and political debate on this issue, and key national strategy and policy documents also draw the boundaries of information sharing more broadly than might be expected given the focus on intelligence and law enforcement data after the 9/11 attacks. A Senate investigative report on the DHS fusion center program (Permanent Subcommittee on Investigations, 2012) quoted extensively from memoranda and plans that were circulated when that program began which framed the information sharing benefits as going well beyond simple "dot collection." These expected benefits included

- Improved information flow from State and Local entities to DHS
- Improved situational awareness at the Federal level
- Improved access to Local officials
- Consultation on State and Local issues
- Access to non-traditional information sources
- Clearly defined information gathering requirements
- Improved intelligence analysis and production capabilities
- Improved intelligence/information sharing and dissemination capabilities

**Figure 1. Modes of Information Sharing Between Organizations**




- Improved prevention, protection, response and recovery capabilities (memorandum from Charles E. Allen to Michael Chertoff, quoted in Permanent Subcommittee on Investigations, 2012, p. 7)

These values are expressed qualitatively and cover both processes (improved information flow) and outcomes (improved situational awareness; improved prevention, protection, response, and recovery capabilities) in general terms. A broader concept of information sharing is also implicit in the 2007 *National Strategy on Information Sharing*, which includes discussion of linkages intended to improve analytic *capabilities* (as well as links designed to share data alone). Such activities beyond "dot collecting" have value, and therefore developing defensible ways to evaluate information sharing must start with clearly defining the different things that these efforts are trying to accomplish. The focus of even post–9/11 sharing programs such as the fusion centers has transitioned from terrorism to a broader all-hazards approach, widening the potential range of functions and information to be shared (Davis et al., 2010).

On the basis of these types of policy documents and other literature exploring information sharing systems and efforts at varied levels inside and outside of government, the present study sought to build a more inclusive set of goals the efforts are seeking to achieve. The intent was to be sufficiently comprehensive that the framework captured most of their intended outcomes but did so within a small number of categories to limit the complexity of subsequent discussion. Four classes of goals were identified that differed in both what was being shared and why:

Such activities beyond "dot collecting" have value, and therefore developing defensible ways to evaluate information sharing must start with clearly defining the different things that these efforts are trying to accomplish.

- **Data sharing.** Data sharing efforts are designed to transmit from an originating organization to a receiving organization specific intelligence or criminal justice data to ensure that the receiving organization has a more complete picture of a person, event, or other relevant entity—the traditional "dot collection" and "dot connecting" goal of information sharing. The intent is to inform a decision or assessment (e.g., about whether a specific person is a threat, what action should be taken in a situation) or increase the chance of a successful outcome (e.g., locating a suspected perpetrator of a crime) in an investigation or other ongoing operation. An example is the law enforcement records sharing systems that can allow a police department in one area to query the information on a suspect known to other departments (e.g., N-DEx at the national level or regional systems like the Automated Regional Justice Information System [ARJIS] in Southern California or the RISS systems). The publication of some types of products from intelligence organizations (e.g., dissemination of current intelligence reports on terrorism from the National Counterterrorism Center [NCTC] on classified information systems) also falls in this category.
- **Notification and alert.** Rather than transmitting individual data on people, places, or activities, some information sharing efforts transmit triggers for action—i.e., from an organization that knows something to another organization that is in a position to act on it—or seek to direct the attention of the receiving agency to a heretofore unknown threat or problem that should affect its actions. Such notification and alert queues up the need for decisions the organization did not know were required before receiving the warning. Examples of notification and alert efforts include interagency threat notifications on which action is expected to be taken (e.g., from federal agencies to local law enforcement). Examples that are less tactically focused include information exchanged in interagency collaboration between social service organizations and the police, where the goal is to inform law enforcement about evolving crime issues in the community. Law enforcement or military BOLO (Be On the Look Out) notifications are also examples of notification and alert sharing. The AMBER alert system that broadly disseminates information on abducted children is another example of a system that acts as a bridge between governmental organizations and the public. Some dissemination of finished intelligence products from intelligence-community organizations (notably warning intelligence) also falls in this category.
- **Knowledge sharing.** A variety of activities are intended not (or not *only*) to share immediate or time-sensitive information but rather to build a common pool of knowledge and lessons learned across separate organizations. Examples include electronic systems for the exchange of after-action reports or interagency social-media systems intended to catalyze direct person-to-person information sharing. The DHS Lessons Learned Information Sharing System (LLIS) and Responder Community of Practice web portals are technological systems that are designed to serve this function. Joint training activities among different organizations are a human-mediated sharing mechanism for educational knowledge sharing, as are processes by organizations to disseminate information for the knowledge benefit of recipients.[10] Systems that share foundational intelligence analytic products (e.g., analyses of countries, regions, or particular topics intended to educate decisionmakers and other analysts) also fall in this category.
- **Expertise sharing.** One goal of some information sharing efforts is linking or bringing together individuals from separate organizations so their interdisciplinary expertise can be applied to common problems. While it could be argued that this is a type of knowledge sharing, it is very different from what is accomplished by exchanging written lessons-learned reports or strategic intelligence products. Linking people and their expertise shares the tacit knowledge and experience held by the individuals involved. The multiagency task forces or centers that collocate personnel from multiple organizations, such as the DHS fusion centers, FBI JTTFs, and joint interagency task forces in the Department of Defense, are prominent examples of this type of effort. Expertise sharing is most effectively done person-to-person, but some technological systems can facilitate the needed connections. Examples include online interagency social media (including the LLIS and the Responder Community of Practice) designed to make it easier to discover individuals with specific expertise. Online collaborative environments such as Intellipedia act not only as nodes for knowledge sharing but also as a means to link the authors of that knowledge for sharing expertise. Information sharing efforts that have significant expertise sharing built in (e.g., task forces, fusion centers, and other multiagency organizations) generally create the capability for acting as a pass-through for expertise or other types of data and also provide analytic value added and filtering as they do so.[11]

These four categories capture the main differences among information sharing activities and the central benefits cited for building bridges between different agencies or individuals working in different security disciplines. While some information sharing efforts focus on only one of these goals (e.g., IT systems designed for very specific sharing functions), others are designed to pursue several simultaneously (e.g., fusion centers or other multiagency task forces that have roles in all four, and IT systems for sharing intelligence across agencies, e.g., the Secret Internet Protocol Router Network [SIPRNet] that have data sharing, knowledge sharing, and warning roles). Neither focus on a single goal or pursuit of several goals is necessarily preferable, although the goals an effort is pursuing should drive how its success is judged.[12]

## Linking Information Sharing to What It Is Intended to Accomplish

Information sharing is generally carried out not for its own sake but for the sake of doing something: Information is shared in the pursuit of a mission. Therefore, measuring its value requires not just identifying what kinds of data or knowledge sharing efforts are trying to share, but how doing so contributes to the outcomes they are intended to enable. Depending on the program and discipline, those outcomes could include detection of terrorist plots and improved law enforcement performance, among others.

The four types of goals identified above can be tied to these broader outcomes by linking them together, since each contributes to different parts of the process of taking raw collected data and using it to inform actions that improve safety or security. The goals are linked in Figure 2, using a hybrid of the classic intelligence cycle[13] and decisionmaking cycles that are used in the organizational-theory literature.[14]

Setting aside data *collection*, since it is outside the scope of a discussion focused on information *sharing*,[15] the process of sharing and utilizing shared information can be viewed as having four main steps (clockwise around the inside of Figure 2):

- Collocating data for analysis
- Identifying *relevant* data in all the available data
- Understanding what the data mean through analysis, often in context with other data, to produce information
- Acting appropriately on the basis of all the knowledge available.

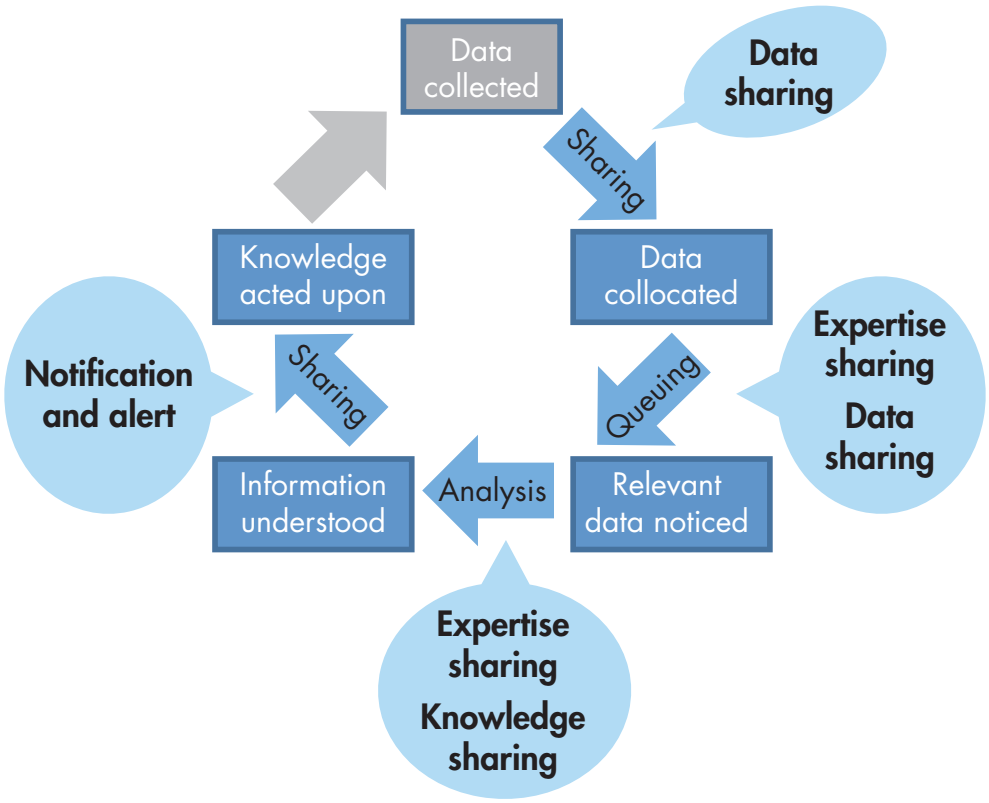
Each step of this process can be viewed as a probability; i.e., the overall probability of "success" is the product of the probability that all available data on a person, crime, or threat will be in one place so the dots can be connected;[16] the probability of recognizing relevant data among the noise of irrelevant data; the probability of understanding their implications correctly; and the probability of acting on the data quickly enough that their value can be realized.[17] As a result, assessments of the value of information sharing must capture the product of all the steps, rather than focusing on individual steps in isolation.

The different types of information sharing discussed earlier make different contributions around this cycle (identified next to each step in Figure 2). In some cases, where the step in the figure is a sharing process itself, the contribution is simple and direct. In others, where what is shared improves the effectiveness of another process, the contribution is indirect:

- *Collocating data* is clearly aided by systems or processes that share data, arguably the function most closely associated with information sharing activities.
- *Noticing relevant data* among the broader pool of noise can be aided by the technical design or features of data sharing efforts (e.g., a system that filters what it shares to increase the chance recipients will not miss important details) but can also be aided by expertise sharing, since specialized knowledge can be required to understand why particular data are important.[18]
- *Understanding* information—analyzing shared data and determining what they truly mean—can be improved by both expertise sharing and knowledge sharing, since knowledge sharing provides analysts or groups with the skills (expertise) and context (knowledge) needed.
- *Acting on finished knowledge,* which often requires moving "finished products" of analysis or warnings gleaned from intelligence information to the organizations that can make use of them, can be aided by notification and alert activities or systems that are essentially conduits specifically for the final stage of the cycle.[19]

Although this sort of cycle is frequently thought of in terms of threat detection—where the action taken is focused on disrupting an attack in progress—it applies similarly to other activities. For example, knowledge sharing focused on disseminating information about past response operations could inform analysis and actions taken to alter planning for future events in an effort to improve performance.

**Figure 2. A Multiagency Intelligence/Decision Cycle Linking the Goals of Information Sharing**




## Lessons from Other Fields on Linking Information to Decisions and Outcomes

Linking sharing efforts with the relevant portions of the cycle sets up the key issue for evaluation: how to measure the contribution of sharing efforts to outcomes the organizations (and individuals within those organizations) accessing the data or information are trying to achieve. It doesn't matter whether a data sharing system shares a lot of data if organizations cannot use the data to improve outcomes. But, particularly for sharing efforts early in the cycle, making the linkage to outcomes can be difficult.

When a specific piece of shared data triggers an action that would not have been triggered in its absence, the effect of the sharing effort is relatively clear. But in many cases, the effect of sharing information is more subtle: Data from one information sharing activity are combined with other data and with knowledge the participants already had, and a decision is made or an action taken. It is difficult to disentangle the effect of the data shared from one system or activity versus other data. There is also a "counterfactual problem": Even though a piece of information might have flowed through a specific system, it does not necessarily follow that in the absence of that system, the information would not have traveled a different path to a similar outcome. As illustrated in Figure 1, a range of information sharing mechanisms exist, and similar (or even identical) information can—and arguably should—move through more than one.

Given the importance of information for making decisions in a range of fields and activities, an extensive literature has examined the value of information and data sharing; that literature provides a starting point for addressing evaluation problems. Early on, research in economics examined how the value of different kinds of information could be assessed in the context of business decisions, since tradeoffs have to be made between the costs involved in collecting and processing additional data and what those data are worth. Techniques used in the economics literature include attempts to quantify how additional information improves decision quality (McCarthy, 1956; Feltham, 1968) and the use of "options thinking" to describe how information changes the relative values of different choices that could be made and the awareness of available choices (Conrad, 1980; Felli and Hazen, 1997). Outcome measures in business are also relatively clear, focusing on how information

affects decision quality and, through better decisions, monetary profits.

Because of the importance of intelligence in military decisions, the value of information in the military context has been a subject of operations research for many years. That research has sought to develop measures and metrics that link information quality, consistency, currency, and other variables to outcomes of military actions (see Darilek et al., 2001, and references therein) and to assess the value of connectivity and therefore sharing of information (see Perry et al., 2002, and references therein). Operations research has also investigated how involving increasing numbers of decisionmakers—and therefore different types of expertise—affect decision quality (see Perry and Moffat, 2004, and references therein).

Studies have also examined specific issues of information quality for decisions, ranging from how value changes given volatility in the environment (e.g., Behrens et al., 2007) to how the value of information coming from multiple sources shifts depending on how independent the sources truly are—a key issue for intelligence, security, and crime-related information in many cases—and the effect of information quality on decisions (e.g., Feltham, 1968; Clemen and Winkler, 1985).

The literature on assessing the value of information and expertise in decisionmaking highlights key tradeoffs in thinking through evaluation and emphasizes the "Goldilocks quality" of many of the issues around information sharing: In most cases, both too little and too much information can create problems, and the goal is to find the level where the data and information served by a system or activity are "just right." An extensive literature can be boiled down to a relatively small number of commonsense observations that highlight the complexities of evaluation throughout the stages shown in Figure 2:

- In many cases, more information is better, particularly if a very high-leverage piece of information (e.g., a key fact or data point) is missing. But too much information can be bad, because of the very real potential for information overload, where valuable data hidden in a sea of irrelevant noise are likely to be missed.[20]
- Conflicting information hinders decisionmaking, but if a conflict arises because of a clash between prior assumptions and new information that demonstrates those assumptions are wrong, the new information is invaluable. Additional information that confirms what is already known can also be useful unless it comes from non-independent sources and essentially provides false confirmation.
- Involving more individuals with different backgrounds in analysis and decisionmaking brings more capabilities and expertise to bear but also increases the complexity of the process, and adding too much complexity can slow the process down significantly.

This "not too little, not too much" dynamic clearly complicates assessment of the value of information sharing. Taking an extreme case, a single-minded focus on improving the probability that all relevant data are shared and available by sharing everything as quickly as possible simultaneously maximizes the chance of information overload and the possibility that important data will be lost in the noise. Sharing everything also maximizes the chance that conflicting data will be an impediment to analysis and decisions, but conscious filtering of what to share and what not to (seeking to eliminate lower-credibility data, limit the chance of multiple reports from the same source being viewed as independent, etc.) creates the possibility that an important piece of data will be discarded. The cost of false positives must also be captured. If inaccurate shared information triggers unnecessary action that would not have occurred otherwise, the cost of that action (which could be paid in dollars or in reductions in public trust, infringements of individual rights, and damage to the reputation of security agencies) must be accounted for and treated as a discount in the value of any successes. The value of information sharing is greatest between the extremes, where the best tradeoff is made between the positive and negative effects.[21]

## HOW HAVE INFORMATION SHARING EFFORTS BEEN EVALUATED TO DATE?

In some portions of the recent political and policy debate around information sharing, DHS in particular has been singled out as having devoted insufficient attention to evaluating whether its sharing efforts—and the fusion centers in particular—have been achieving their goals. The 2012 Senate report cited repeated unsuccessful attempts by congressional overseers to get information and data on fusion center performance and criticized DHS efforts (or lack of efforts) at developing defensible measures of performance for the program (Permanent Subcommittee on Investigations, 2012, p. 8, fn 19). It summed up the committee's frustration, saying, "DHS has not attempted to conduct a comprehensive assessment of the value federal taxpayers have received for [their] investment [in state and local fusion centers]" (Permanent Subcommittee

on Investigations, 2012, p. 6). The Government Accountability Office (GAO) has raised similar questions about DHS and some of its components, the ISE, and other federal information sharing efforts since 2001 (e.g., GAO, 2008; 2010a; 2010b; 2011; 2012).

Although there are many legitimate criticisms of past efforts to assess the value of information sharing activities, it would be incorrect to conclude that no such efforts have been made. Over decades of effort, policy and evaluation researchers have developed structured ways of looking at the effects of programs (not only information sharing efforts) and attempting to assess their value and effectiveness even when exactly what they are accomplishing is difficult to measure with certainty. Such methods include examining measures to assess *process* (whether a program is being put in place or functioning effectively), *output* (what products or services the program is producing directly), *outcomes* (how what the program is producing affects the accomplishment of the desired goals of the organization), and *efficiency* (whether the costs of what is being produced are higher than those of other ways of producing the same outcome).[22]

In the literature, there are a number of examples of efforts to develop measures and metrics to assess information sharing and related activities. Prominent among these are systematic efforts to assess law enforcement computerized information sharing systems, given the investments that have been made in such systems for many years. Two such examples illustrate the construction of measures at a very detailed level:[23]

- *Performance Measurement for Justice Information System Projects,* published by the Bureau of Justice Assistance. This manual identifies 24 outcomes that criminal justice information technology could contribute to achieving, ranging from reducing gun violence to improving the functioning of court systems. It provides examples of output, efficiency, and outcome measures for subsets of those outcomes in a variety of project types (Center for Society, Law and Justice, 2008).
- "Implementing Regional Law Enforcement Information Sharing Systems" (Center for Criminal Justice Technology), a report that provides extremely detailed measures for all parts of an information sharing system, including process measures (e.g., times to access services, availability, data accuracy), output (e.g., amount of data delivered, number of queries run), outcome (e.g., arrests resulting from system use, leads identified), and efficiency (e.g., time saved by using the system). The analysis provides 80 individual measures for assessment, many of which include multiple, more-specific submeasures (Noblis, 2007, pp. 3-3 through 3-7).

However, the fact that more information feeding an organization or decisionmaker can produce both positive and negative effects creates problems for traditional evaluation efforts that move from (generally) easier-to-assess process measures to (generally) more-difficult-to-assess outputs or outcomes (Bureau of Justice Statistics, undated(a)).[24] Indeed, these systematic efforts at metrics development show both the promise and the peril of information sharing program evaluation. While it is possible to frame clear outcome measures for such efforts and detailed measures for process and outputs, measurement and ascribing clear effects to the systems or initiatives sharing the information can be difficult. Traditional process measures like system availability and ease of use are clearly relevant, but process and even some output measures could also produce confusing and potentially nonsensical conclusions. Measuring increases in data delivered by an initiative (a process or output measure for the sharing effort) is an improvement if the data are the *right* data, but if the data are not valuable, such an increase could be a measure of a negative effect on the mission outputs or outcomes of the organization receiving the information.

Although process and output measures can provide insights into how programs function, outcome and efficiency measures are of more interest, since information sharing is an intermediate activity being done to achieve mission goals. Linkages to outcomes are also critical for assessing information sharing systems that are aimed at different goals (or combinations of goals). Systems that share data and initiatives that link organization members to others with the expertise needed to use those data well are very different types of information sharing, but both are designed to improve the outcomes the organization can achieve. Without getting to outcomes, the potential to undervalue or overvalue elements of a sharing initiative that fall differently across the four categories of goals described above is significant.

Information sharing in policing provides a straightforward example of this dynamic and illustrates the importance of tying evaluation to desired outcomes. One output or outcome measure[25] frequently discussed in policing is the making of arrests to clear outstanding crimes. Given the broader goal of enforcing laws fairly and safeguarding the civil liberties of the populations that the police are charged with protecting, a more specific construction, *quality arrests*—arrests that lead to prosecution and/or conviction—are also used as a measure. Because

These systematic efforts at metrics development show both the promise and the peril of information sharing program evaluation.

the decision to prosecute (and success in doing so if a case is taken forward) is related not only to the occurrence of an arrest but also to the quality and amount of the evidence supporting it, quality arrests can be a better measure for desired outcomes than simple arrest counts alone.

Many information sharing efforts could deliver information to police officers that could affect their arrest behavior:

- Systems that provide data on outstanding warrants for individuals in other jurisdictions increase the chance the offenders will be picked up when they interact with police (e.g., in a routine traffic stop). But if the data are old or incorrect (e.g., outdated warrants that have been resolved and should have been purged), the increase in arrests might actually decrease the rate of quality arrests.
- Biometric and biographical information can help officers see through attempts by individuals to deceive them about their true identities, limiting the suspects' ability to evade arrest. But bad or too much data could produce the opposite effect, resulting in people picked up for the wrong reasons.
- Knowledge sharing systems that educate officers and reduce the chances of procedural or policy failures that could enable otherwise legitimate arrestees to gain release could be reflected in an increase in arrest quality. But sharing systems that provide interesting information that is of limited mission utility could result in officers spending more and more time simply "keeping up" with the systems' output and spending less time on the activities that result in arrests and crime clearance.
- Investigative systems that provide more leads to follow up could produce more and better evidence that increases the probability of arrests leading to prosecution and conviction.

Maintaining focus on the true end result desired—not just arrests but *quality* arrests—internalizes these tradeoffs and the potentially mixed effects of information in general and focuses on the effects of a specific effort on organizational performance. A comprehensive, strong example of evaluation approaches that address the full criminal justice process, from inputs through desired outcomes, is the approach of Rhodes et al. (2009b), which examines evaluation of multijurisdictional task forces for drug enforcement.

The following sections review representative assessments of process and, where available, outputs and outcomes, using (occasionally) directly measured, quantitative data and (more frequently) mixed-methods approaches often based on indirect, qualitative assessments such as judgments about outcomes by users. An important caveat for such an examination is that not all of the assessment that is done is made public, so this review is necessarily limited to studies and results that are publicly available. However, given the focus on what is needed to inform public policy debate on these programs, it could be legitimately argued that the public component of such data and research is the most relevant information.

## Examples of Direct Measurement of Information Sharing Process, Outputs, and Outcomes

The annual report of the federal ISE (along with the information available on the ISE web site) is a prime example of direct, quantitative measurement of information sharing *processes*. The web site includes data on the content of the CJIS databases (numbering in the millions of records), transactions per day, average response times to queries (measured in fractions of a second to minutes), and system availability. The 2012 annual report included a variety of activity statistics that track the process of information sharing, including agency participation in different entities such as fusion centers, suspicious-activity reporting (e.g., questions about whether the agency trains for such reporting, maintains a database, etc.), and broader infrastructure issues such as interagency agreements and adoption of standards. The GAO has observed that most attempts to measure information sharing activities at the federal level have this character, with a focus on process measures over measures that assess whether the activities are achieving their desired outcomes (e.g., GAO, 2010b) and sometimes limited planning

to improve measurement in the future (e.g., GAO, 2010b; 2011; 2012). Efforts to assess the fusion centers in 2011 were similar, focusing on quantitative measures of process (e.g., whether plans were in place, positions staffed) rather than on outputs or outcomes (DHS, 2012).

Direct quantitative measures of outputs or outcomes are quite rare in the available public literature. Information sharing systems with very well-defined (and narrow) goals—e.g., the systems surrounding the national No Fly List, where dissemination of names rapidly enough to keep individuals off planes is the desired outcome, or RISSafe, a database focused on deconflicting police undercover operations—are more straightforward to assess quantitatively in this way, since there are few substitutes for data they provide, and their effects are readily countable (BJA, 2012). Buried in policy-type documents are occasional data-based assessments that link increased use of an information system quantitatively to outcomes. For example, buried in the Bureau of Justice Assistance 2010–2012 Strategic Action Plan (BJA, 2012) is the following description of a change that made using an information sharing system easier and linked that change to significant increases in usage and changes in outcomes:

> The state of New Jersey also implemented a technical solution to make the submission easier. The NJSP developed a program that automatically populates the eTrace fields from the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC) submission. Within a 6-month period, compliance rates were increased from 9 percent to more than 85 percent, and more than 15 indictments occurred as a result. Five states in the same region, as well as ATF, would like to replicate the New Jersey approach. Leveraging these sites will improve state gun-tracing efforts and establish collaborative relationships across state lines. (BJA, 2012, p. 8)

Such clear-cut examples are relatively rare, and quantitative measures for systems whose outcomes are less clear-cut are even less common. The use of anecdotal success stories has become a common feature in the policy debate surrounding these systems. Such exemplary data points can be found in national-level reports (e.g., ISE, 2012, p. 8), Department web sites (e.g., DHS, undated) provided as evidence to congressional examiners (Permanent Subcommittee on Investigations, 2012, p. 83), and practitioner assessments of efforts (e.g., Davis, 2013).

Such anecdotes, however useful they might be as illustrative cases, are not a sufficient basis for assessment, as they suffer from unavoidable selection bias—i.e., they are not as clear a direct measure of the system's effects as they might seem—and they never address the full picture of how the sharing efforts perform. The 2012 Senate report on fusion centers demonstrated how such anecdotes can be reinterpreted in the course of policy debate, making the validity of the data as much a point of contention as what the data say or do not say about the value of the program at issue (Permanent Subcommittee on Investigations, 2012, pp. 96–105).[26] Other examples are available in the literature: Researchers at Noblis examined several regional law enforcement information sharing systems during an effort specifically focused on metrics development for these activities. Their case studies included only limited efforts to assess the effect of the systems, with the exception of "success stories" and getting users to provide qualitative feedback on whether the systems resulted in additional leads, arrests, or other outputs (Noblis, 2007).

A notable example of an attempt at quantitative evaluation of an information sharing system was that of Hauck (2005), who examined a communications application that was part of a department's computer-aided dispatch system (essentially a law enforcement instant-messaging application). Hauck sought to link use of the tool to measures of individual officer productivity such as number of arrests and number of cases where the individual was the primary offender. Results from the analysis were mixed, which is unsurprising given the nature of the communications tool being assessed and the range of its uses (in contrast to, for example, the simpler information sharing application of a remotely accessible database).

Between 2000 and 2010, a substantial research effort was directed at the evaluation of multijurisdictional task forces, a central function of which is promoting information sharing between participating organizations (an example of multiagency organization, as shown in the center right of Figure 1). One team of researchers performed a substantial literature review early in this effort, examining the evaluation that had been done on these task forces at that point. Their conclusions echoed those of the present literature review, i.e., that most of the available studies focused on process evaluation and examining how programs were implemented. A smaller number of evaluations documented quantitatively measureable outputs, including the number of arrests and convictions that could be linked to the task forces' efforts. Some of those studies were essentially descriptive, although some used stronger methods (e.g., pre-post measurement). Another subset of the studies looked at effects at the organizational level, comparing outputs between participating and nonparticipating organizations. These studies produced some measures of the effect of task

force participation on outputs such as drug arrests. A smaller number of studies looked at final outcomes, e.g., assessing community impacts such as reductions in drug use or drug-related crime. While most were descriptive, some used pre-post or time-series designs to assess broader outcome effects (Hayeslip and Einhorn, 2002).[27]

In subsequent research, one team examined existing practices at task forces for evaluating their own activities, designed an evaluation, evaluated several task forces (focusing on a defined set of data elements: "task force jurisdiction, partners, FTEs [staffing levels], operating budget, investigation activity, arrests, eradications, and seizures") and developed evaluation tools to assist others (Rhodes et al., 2009a, p. 4). Significant data gaps at the task forces being studied for the seven-year window selected for their retrospective assessment and variations in the quality of data that were available complicated analysis, but time-series analysis of how changes in inputs affected outputs and outcomes was done (Rhodes et al., 2009a). Other contemporaneous evaluations of task forces identified other innovative ways of evaluating their efforts, including comparison of the characteristics of the offenders arrested and prosecuted by participating vs. nonparticipating organizations (Olsen et al., 2002). Information sharing is a central part of these task forces' functioning, but they also perform a variety of other functions, which creates the additional complication of disaggregating the part of their outputs or outcomes that can be ascribed to sharing.

## More-Indirect Assessments of Information Sharing Process, Outputs, and Outcomes

Though solid quantitative assessments of information sharing activities are sparse, a variety of efforts have been made—in both the policy and academic communities—to use mixed methods, often qualitative approaches, to get some insight into the systems' and efforts' value. These approaches can use quantitative tools; in fact, the most systematic of them have involved the use of self-report user surveys that ask questions about the *perceived* value of activities and their effect on outcomes. However, because the surveys ask questions about perceived value, they provide results that are quite different from truly direct assessments of the systems. In such cases, the strength of the result lies in the rigor of the survey or data-collection process, with significant variation from assessment to assessment. For example:

- In its annual reporting, the ISE presents data on the perceived value of some information sharing initiatives, including federal-agency respondents' perceptions of the "extent access to terrorism information has improved" and the extent to which the agency's "ability to discover, assess, and retrieve information needed to accomplish mission" has improved. The ISE also asks questions about efficiency, such as perceived time savings from improvements in information sharing (ISE, 2012).
- Zaworski (2005) carried out an evaluation of ARJIS, a regional information sharing system in Southern California. He sought to identify the effects of the system by comparing an ARJIS-connected agency with a similar agency in another part of the country. The ARJIS users reported perceived improvements in their ability to make arrests, clear cases, investigate crimes, and perform other police functions. However, comparison of the qualitative results with actual data from the two agencies (in this case, combining indirect measures with more objective, directly measurable data) suggested a different conclusion, since the ARJIS agency appeared to perform worse than the comparison agency in arrests, particularly for property crimes. In seeking an explanation for the counterintuitive result, Zaworski identified clear differences in culture and management practices between the two departments, as well as significant differences in the amount that officers used their computers. This effort demonstrated the challenges in evaluating information sharing given the difficulty of effectively controlling for other influences.
- The literature contains self-report user evaluations of the perceived value of different information sharing systems

Anecdotes can be reinterpreted in the course of policy debate, making the validity of the data a point of contention.

and activities. Examples include a self-assessment of the COPLINK Connect system reported by Chen et al. (2002), which asked whether the information provided by the system was useful to the respondents and whether it improved their productivity and job performance. Another evaluation asked similar questions of users of Florida's FINDER system (Scott, 2006).

- Bean (2009) sought to examine relationships between use of an information sharing system and other variables to assess the effects of the system through a survey of users of DHS's LLIS. The sample survey showed some relationships between use of the system and increased awareness of threats and perceived job effectiveness of the respondents, but the methods were such that it is difficult to generalize from the results. Other examples of small-sample-size surveys include Odabasi (2010), who examined law enforcement acceptance of fusion center systems, and Dethlefs (2003), who studied the use of federal information systems.
- Given recent attention in the policy debate, examples also exist of efforts to evaluate fusion centers. Rojek et al. (2010) used survey methods of users of the South Carolina Fusion Center to assess awareness of the information shared by the center, asking respondents whether they used the information and how they perceived its usefulness. Carter and Chermak (2012) carried out a broader self-report survey of fusion center representatives that primarily assessed process measures for the fusion centers' activities. The survey included assessments of participation and working relationships across different agencies, the likelihood that participants would consult with people outside their own organization, linkages to various technical sources of information such as databases, and the interaction of the fusion center with its users to improve the quality and usefulness of the information shared.

These relatively limited systematic qualitative studies are complemented in the policy literature by the qualitative version of "success anecdotes" (discussed previously). For example, the aforementioned Senate report on fusion centers (Permanent Subcommittee on Investigations, 2012) raised concerns about the utility of the information being shared, based on broad estimates of the fraction of shared data that was not useful.[28] Critical comments about "sharing too much" have been echoed in other qualitative analyses, along with the need for "humans in the sharing loop" to act as filters for what information is shared and what is not (Bean, 2009). This latter need is echoed in some policy documents as well (e.g., PM-ISE, 2010).[29] Other sources draw on similar interview-based data to characterize the sources of information in some information sharing processes and the extent to which they produce new analysis rather than repackaging other information (e.g., Carter and Chermak, 2012, p. 73).

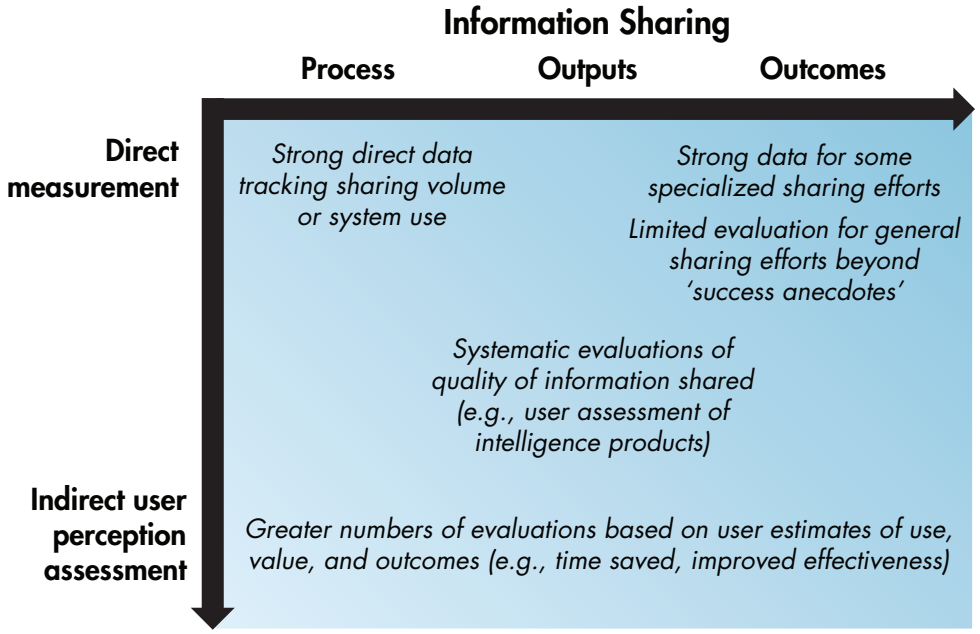
### Insights from—and Blind Spots of—Available Evaluations

The evidence base produced by past evaluations of information sharing efforts is quite weak. Figure 3 summarizes the strength of existing studies, with movement from left to right showing available data on process through outcomes, and from top to bottom from the strongest, directly measured data to indirect assessment approaches. Although strong direct data are available on processes (as would be expected given the ease of measuring things like daily transactions in sharing systems), data on the outcomes of these systems are available only in rare cases. Hybrid efforts focusing on outputs (e.g., evaluation of the quality of information shared) fall in the middle of the spectra, combining direct measurement with user perceptions of value.[30] As a result, most existing assessments of outcomes—addressing the fundamental questions of whether information sharing is saving agencies time or money or making them more effective—rely on user perceptions. While such indirect assessment is better than no evaluation,[31] user perceptions are not sufficient to provide definitive results given the real—and contentious—policy debate on the value of these efforts.

## ARE THERE BETTER WAYS OF EVALUATING INFORMATION SHARING AND FUSION EFFORTS?

Given the four main classes of activities that frequently fall under the general rubric of information sharing, are there better ways to assess such efforts to judge whether their value justifies the resources being devoted to them? Drawing on the examples from past analyses and the broader criminal justice and homeland security literature, a variety of evaluation needs can be identified, along with a broader set of propositions and hypotheses about how those needs might be met and some concrete analytical directions that appear particularly promising.

**Figure 3. Strength of Existing Evaluations of Information Sharing Efforts**




## Evaluation at Implementation Versus Post Hoc Assessment

Addressing the problems in evaluating information sharing systems begins with the simple but important point that assessing a system that is already in place and being used is a different task from assessing a change in information sharing as the system is being implemented. In the latter case, there is an opportunity to determine specific data required to evaluate the effects of the system, make measurements before the system is put in place, and then compare that baseline with later performance. Even more sophisticated designs may be possible to further isolate the effect of the sharing system. Such designs might incorporate features such as randomized treatment groups (i.e., a subset of an agency that is given access to the system) and controls (a subset that is not given access until later).[32] Evaluation efforts to assess a system that is already in place do not have these pre-implementation options, making the creation of control groups for comparison more difficult.

Potentially more important, planning for evaluation as a system is implemented also improves the likelihood that the data needed will be captured at all.[33] These issues apply to all four of the classes of sharing efforts discussed previously, but they may be particularly problematic for expertise sharing efforts, which are frequently person-to-person activities and are thus potentially the least likely to automatically produce analyzable information for assessment. In view of this, evaluation methods are needed to assess the value of the many investments in information sharing that have already been made, in spite of the greater difficulty of doing so. Future information sharing investments could have evaluation requirements and resources built into the programs to provide the greatest potential for limiting the risk that a focus on implementation alone will make the value of the investments difficult to assess.

## Considering Stock Effects and the Value of New Information Sharing Initiatives

There is clearly potential for a "stock effect" resulting from an organization's existing endowment of other information sources and sharing linkages. The expected effect of adding an agency's first information sharing system or activity could be quite different from the effect of adding its tenth. If the new resource overlaps with existing information sharing connections, it will represent an incremental improvement almost by definition. In contrast, for an organization with only its own resources to rely on, the first new information sharing system could have a much larger relative effect. Therefore, evaluation approaches must go beyond focusing on the system as the unit of analysis, since the larger information context within the agencies where any system is implemented will significantly shape its value.

This issue will play out differently for the different classes of information sharing defined previously. For data, notification, and knowledge sharing systems, overlap versus new capability will be mostly a function of understanding what those systems share versus what is already available. For expertise sources, the central driver will be an existing organization's internal capacity and what is available from partners it routinely works with. In both cases, the issue of whether the new effort increases the possibility of information overload or transaction costs (i.e., the need to consult or use an additional system) will also drive whether "new capability" really represents an increase over an agency's baseline.

## Caution in Focusing on Process Measures Rather than Outcome Measures

The traditional program-evaluation approach of building from measuring processes or outputs—internally focused metrics of the individual program (see Noblis, 2007)—to more important and valuable outcome measures is risky for information sharing systems in ways that it is not for many programs. Since information sharing programs are designed to enable organizational success in other, often very different activities, process or simple output measures of the sharing activity itself can produce pathological results. For example, process measures of an initiative that broadly shares bad data and does so very rapidly might make the initiative look very good—large numbers of users, high usage, many reports produced, etc.—but these factors could be impeding rather than aiding the organization's actual performance. Anecdotes can be found about the sharing of bad data and the negative outcomes it can produce, but understanding of how to measure its costs is lacking. To be truly meaningful, the crux of evaluation must be assessment of effects on organizational outcomes and mission success. For example:

- For a tactical data sharing effort in a police department, the outcome of interest is the way arrests (or the probability of prosecution and conviction given an arrest) change based on the availability of more data from federal or other jurisdictions' systems.
- For a system that shares intelligence data with analysts, measures of changes in the quality of the analysts' products—which could range from individual measures based on a review of content to more academic measures such as how frequently their work is cited by others—would be appropriate.
- For knowledge sharing activities, like those of the many systems that push finished intelligence products out to potential readers, the outcome measure of interest is how exposure to those products affects decisions (measures like numbers of readers and downloads are only somewhat meaningful in the absence of such insight).
- For expertise sharing efforts, understanding the degree of contribution that others outside the organization make to its analytic, decisionmaking, and other activities—and how important the contributions actually are—would be the goal of assessment.

Linking system usage and the information provided to organizational outcomes is the only way to assess value in relation to costs (both the initial costs of the sharing effort and the sometimes considerable resource and time costs of sustaining the effort over time by both agencies sharing their data and users and receivers absorbing the information provided).

Measuring changes in organizational outcomes is clearly difficult for systems whose goal is the prevention of rare events, as is fortunately the case for efforts focused on the prevention of domestic terrorism. In such cases, the number of annual events is small enough that changes attributable to new information sharing would be difficult to detect statistically. As a result, the current practice of focusing on success stories where shared information played a part is necessary but not sufficient to demonstrate the value of the sharing effort. To substantiate the value of the effort in the success, a second step is needed—what the Center for Society, Law and Justice labels "but-for" measures:

> These are measures that count outcome events that could only have occurred with project technology. For example, a new crime-solving technology, such as DNA testing, might have as an outcome measure the number of crimes solved with the technology *that would not have otherwise been solved*. Capturing these measures might require a case-by-case analysis where the technology has been used and often involves judgment calls. In some ways these measures are more powerful and convincing indicators of the technology's impact than other options, because they can eliminate alternative explanations for change. (Center for Society, Law and Justice, 2008, pp. 13–14, emphasis added)

Looking at the range of different possible information sharing paths shown in Figure 1, "but-for" analysis of an information sharing activity must address the likelihood that the data, notification, knowledge, or expertise that was key to the success would have been shared in other ways and, if so, whether those ways would have been rapid and efficient enough to have also produced the success. Such analysis seeks to fairly weight the

> Linking system usage and the information provided to organizational outcomes is the only way to assess value in relation to costs.

individual data points provided by success stories, giving high weight to success that *would not have occurred at all* without a system or initiative, but not unfairly "putting a finger on the scale" to give the system credit for successes that would very likely have occurred anyway.[34] Such "but-for" examinations could also ask about the incremental effect of a system—e.g., how much faster a suspect was apprehended than he would have been in the absence of the system—although such incremental effects would be more difficult to substantiate and support than cases where the absence of the system would clearly have led to failure. The chain of probabilities shown in Figure 2 can be linked to such an analysis, where the examination of successes and exploring how they might have transpired in the absence of a particular sharing activity provides a way to bound how much the presence of the activity increases or decreases the probabilities of each step.

This focus on outcomes enabled by information sharing should not be interpreted to imply that intermediate measures are of no value. Traditional process measures are clearly useful for those managing an information sharing effort (i.e., if information is being shared and no one is receiving it at all, this would be a concern), even if they do not say much about the effort's absolute value. Some intermediate measures focused on the characteristics of the information flowing through a system or activity can be more closely tied to organizational outcomes and, therefore, value. For example, measures of information quality (e.g., the fraction of information flowing that is demonstratively false, or the false-alarm rate for a notification and warning effort) are tied to outcomes, since the frequent receipt of bad information would generally not enhance any organization's effectiveness. Given the potential for information overload and burdens created on receivers to review shared data, one could also consider a "signal-to-noise" ratio for the effort, i.e., the ratio of the amount of information that is relevant and important to the receivers to the amount that is not. Such ratios would be audience-dependent (e.g., data that would be viewed as signal by an intelligence specialist might be viewed as noise by a senior decisionmaker).

## Different Assessment Needs and Opportunities at Different Levels

Given the range of information sharing efforts that are implemented at different levels, evaluation needs—and, therefore, evaluation approaches—can be framed at different levels of analysis. Evaluations can be based on where outcomes are intended to accrue, from the national level down to a much more detailed or local level. That said, the borders between the different levels blur, driven in part by the fact that these systems are, often by definition, designed to bridge such divides.

### *National-Level Evaluation*

Most of the information sharing systems whose effects are intended to manifest at the national level are designed to disseminate intelligence information among or within agencies at the federal level. The outcome of interest for these systems is whether shared information has a positive effect on the national security of the country as a whole. For a single country, this is almost the epitome of an evaluation question where there can be no control group for comparison. Even if friendly countries were sufficiently open with one another that they could be compared in this way, differences in systems and processes would almost certainly make the results insufficiently comparable to be meaningful.

How, then, can the value of a system or initiative that an intelligence organization has put into place or the value of the suspicious-activity reporting that flows upward to the national level through multiple homeland security and law enforcement systems (GAO, 2013a) be assessed? A good starting place is a simple assessment of duplication, a concern that has been raised by congressional overseers about some existing systems (GAO, 2013b). Duplication can exist either at a high level (e.g., two systems designed to do essentially the same thing) or at more detailed levels (e.g., although intended to be distinct, the actual data shared through systems echo one another, meaning that systems that are different in theory are similar in practice).

A duplication analysis is essentially a mapping effort of existing systems and initiatives, with enough detail on their content to allow them to be appropriately compared. This can

be done to a point from the outside but, as shown by a previous RAND effort to map domestic intelligence efforts (Jackson, Noricks, and Goldsmith, 2009), it is much more difficult—for legitimate security reasons—to assess at a detailed level from the outside. "Rebroadcasting" by an information sharing system is not *necessarily* bad (since rebroadcasts could be the route by which information gets to important subsets of users), but the more a system's content mirrors that of other systems, the more scrutiny its costs might receive. Even sharing the same information through multiple channels (e.g., separate systems) to the same audience could increase the probability that any given piece of information is seen, but it could paradoxically increase the risk that the information fails to be noticed or understood given the potential for information overload (Figure 2).

For new information sharing activities, pre-post analyses could be done at the national level, although such efforts would be most readily applied to initiatives that produce regular outputs (e.g., how a new system affects the quality of assessments done regularly enough that change might be detected). For existing systems, if outcome measures can be framed at the national level, can they be defined to correspond to the intended effects of the system? For example, one of the key goals of national crime databases of forensic information (e.g., the Integrated Automated Fingerprint Identification System [IAFIS] database) is to increase the probability that criminals who offend in different jurisdictions will be apprehended via the linking of evidence found at different crime scenes. A recent analysis that took advantage of the availability of DNA evidence in the Netherlands (on both solved and unsolved crimes) demonstrated that repeat crimes by individuals who crossed jurisdictional boundaries increased the probability of apprehension substantially less than repeat crimes within a single jurisdiction (Lammers and Bernasco, 2013). National-level information sharing systems would, in principle, reduce the cross-jurisdictional "advantage," suggesting a measure that could be used to assess the effects of such systems.[35]

How the information provided by different systems is utilized (essentially a process measure) is a readily measurable value, and one that is used in public reporting on some initiatives (e.g., ISE, 2012), but, as discussed previously, use of information from a system does not directly equate to value. Process measures are unambiguously valuable in the negative direction, however, as a sharing initiative whose information is *not* used is clearly *not* contributing to improved outcomes.[36] Any assessment of a system applying positive usage statistics as part of its supporting case must take into account the extent the information used is duplicated in or rebroadcast from other sources. In such cases, the "value added" provided by the system would be less than that of an initiative that shared unique data or products (e.g., by filtering raw intelligence data and sharing only the relevant subset, increasing the likelihood that relevant data will be recognized).[37]

Some information sharing programs that are framed at the national level can also be examined at a more disaggregated level. For example, suspicious-activity reporting is a national program that feeds databases intended to be valuable to federal-level counterterrorism efforts. However, such information is also intended to be utilized by state, local, and tribal law enforcement. As a result, while the effects of the shared information could be assessed nationally (e.g., what access to certain types of information has enabled the FBI or intelligence organizations to do, and how differences in the extent and nature of reporting across the country affect those outcomes), they might also be assessed at an organizational level (e.g., what participation in the effort and use of information shared horizontally or top-down do for the outcomes of an individual metropolitan police department or state homeland security agency). Since these local outcomes are a major part of what the national programs are designed to achieve—in a real way, the national effect of the fusion-center program is the integral of all the effects across the country plus any federal-level effects—evaluating them both in aggregate and as individual components is both appropriate and useful.

### Organizational-Level Evaluation

For national-level programs, such as the fusion centers, or databases like those maintained by CJIS, participation and use by many individual organizations can provide more comparative leverage to assess information sharing efforts. Rather than the system producing a change in one national-level measure or outcome, a system with many subscribers could affect many possible streams of outcomes and could provide a broader dataset in which its effects might be discerned. For example, in a pool of a thousand organizations linked to a database, it might be possible to identify two organizations that are very similar to one another except in the extent they use the database. If the organizations and their circumstances are otherwise identical, it would be easy to make a causative argument that detected differences in performance—positive or negative—came from the use of the information system.

Organizational outcome measures (e.g., crime levels; arrest, clearance, and other rates; specialized measures like cross-

jurisdictional arrests) would provide the basis for comparison if there is both sufficient comparability among participating organizations and sufficient variation in their use of the sharing system. What *differences in use* means at the organizational level is important. Even if two organizations are nominally connected to the same information sharing system, the actual delivery of information to the agencies may differ. A technologically savvy organization might use the system a great deal, delivering data directly to practitioners as they carry out their duties. A technologically lagging organization might be nominally connected but might provide access only at a central terminal and would therefore not actually get much information from the system at all. In these cases, process measures such as users, downloads, searches, and other values become measures of the "relative dosages" of the information sharing initiative in different agencies and also ways to better link outcomes to the enabling effects. Differential-effects examinations would have to take into account potential self-selection issues (i.e., greater use of a system might be associated with more-effective organizations with or without that use), but such concerns might be controlled by time-series analyses that examine how outcomes change for a user as usage level changes over time.[38]

Other types of information sharing could also be assessed this way. In the past decade, a central focus in discussions of information sharing at the state, local, and tribal level has been the ability to provide classified intelligence information to inform decisionmaking (e.g., Kaiser, 2003). Progress has been made in this area, but differences that remain could be used to assess how access to such data has affected different types of organizational performance. "But-for" analysis would likely be critical here, given the rarity of terrorist plots, in which such information would be assumed to be most relevant, but other topics could provide a basis for comparison (e.g., policing transnational crime organizations, where such data might also be relevant).

In doing these sorts of assessments at the organizational level, both the "stock effects" discussed above and a different variant of such effects could shape performance. In addition to the value of a new initiative at the organizational level being affected by its existing stock of information, the stock of data in the sharing effort itself would also logically affect how outcomes are manifested. Regional information sharing activities where multiple organizations contribute data to a communal effort provide the best example of this potential effect. Such activities may have a critical-mass effect, where the value of the system is low when only a few agencies provide data but increases rapidly as the number of participants increase and therefore the amount and diversity of data available increase. In such cases, technology-adoption assessments (e.g., Skogan, et al., 2003; Skogan and Hartnett, 2005) need to be a part of system-value assessments, since linear changes in numbers of participants (e.g., from two agencies to four or six to eight) might produce nonlinear changes in value.

Rather than seeking organizational-level effects by looking across many agency participants in single information sharing systems, it is possible to examine effects at the individual organizational level. Evaluation in the course of implementation or through pre-post analysis can produce useful results, as the New Jersey pre-post data cited previously showed (BJA, 2012, p. 8). But in other cases, such efforts are essentially case studies and to the extent that they can be quantitative, must rely on matching the case organization and its exposure to the information sharing to another similar organization without that same exposure. Making that match can be difficult, as was clearly demonstrated in the evaluation of ARJIS, where it became apparent to the evaluator in the course of study that the comparison agency differed in important ways other than its access to information sharing (Zaworski, 2005). Use of objective measures like the number of cross-jurisdictional arrests could provide a lever for quantitative components, but such measures are not always available.

The focus here on quantitative outcome measures for information sharing—the key to substantiating the cost-benefit

Rather than seeking organizational-level effects by looking across many agency participants in single information sharing systems, it is possible to examine effects at the individual organizational level.

of such systems—should not be interpreted as a dismissal of other value that detailed case studies can provide, even if they cannot make clear outcome linkages. For example, examination at the organizational level can provide detailed qualitative insights into how the effects of new information sharing initiatives are occurring and can therefore help in understanding any observed outcome effects. In a case study of a Los Angeles County information sharing system that was designed to limit officer use of the radio—keeping the "air clear" for priority traffic—it was observed that some officers were using the system to simply replace the situational awareness that they had previously gained from listening to others' transmissions over the radio. That is, while it achieved the goal of clearing radio channels, the change produced an information sharing deficit that had to be made up before it could show positive outcome effects. Without such a case study establishing the existence of such an effect, quantitative outcome data might have been misinterpreted (National Consortium for Justice Information and Statistics, 2009, pp. 3–4).

### *Micro-Level Evaluation*

If evaluative resolution could be gained by moving from assessing the effect of information sharing nationally to assessing how different organizational subscribers to a single sharing initiative performed, might more leverage be gained by moving to a still lower level? Use of information sharing resources varies within single agencies. Some variation is driven by role (e.g., within a police department, crime analysts would be expected to use different information systems than detectives, and both would use different systems than patrol officers). But other variation within roles could arise simply from the different ways individuals choose to do their jobs, or from variation in the amount of technical orientation of specific individuals, or in habits of using different substitutes for the data or expertise coming from information sharing initiatives.

Such differences in use, which could result in different levels of exposure to the sharing effort that could be tied to individual-level outcomes, would vary among the classes of information sharing systems. Knowledge and data sharing systems would be expected to have such differences (since much of their use occurs at the individual level), while notification/warning efforts would not. Expertise sharing efforts could have differences depending on their implementation, although they could also act more as organizational than as individual-level resources (e.g., organizational participation in a fusion center versus individuals within the organization having access to the different experts within the center).

If such differences do exist, assessment at the individual-user level could be particularly effective for evaluating information sharing efforts that are already in place. This was essentially the strategy of Hauck (2005), whose analysis attempted to relate differences in the way individuals used a communication system to police-officer-level outcome variables such as arrests and arrest quality. The larger number of individual users within systems could enable the use of more-sophisticated techniques for matching of individuals who are similar (e.g., in role within the organization, tenure, specialization) but differ in the amount they utilize information sharing tools. This could make linkage to individual-level outcomes for operational practitioners (e.g., patrol officers, detectives, certain military officers) or analysts (e.g., crime or intelligence investigators) more straightforward. Correlations between information sharing resources and such outcome variables could more readily support causative arguments the more similarly individuals could be matched, and the effects could then be built "back upward" to aggregate estimates of the effect of the initiatives on organizational- or national-level outcomes. As was the case at the organizational level, self-selection concerns would have to be addressed (e.g., if initially more-productive members of the organization were more likely to be heavy users of the system, their baseline difference in expertise could be misunderstood as resulting from the information sharing system). Time-series analyses examining variation in individuals' use and performance could provide a way to control for such differences, as could other measures of individual users' expertise or skills.

## CONCLUSIONS

The investments made in information sharing efforts in the years since 9/11 have created a clear need for ways to assess the value of the initiatives and weigh their costs and benefits. In addition to the costs associated with establishing new sharing efforts, such activities—particularly those involving significant personnel commitments and resources—can have significant sustainment costs as well. Beyond comparisons of their costs and benefits, these programs have also raised significant questions about who should pay the costs. Federal investment has been justified by the contribution of information sharing efforts to broader national security goals, concurrent with other federal

programs designed to support state, local, and tribal jurisdictions. But arguments for support at the subnational level also can and have been made, arguments in part shaped by assumptions about the nature of the benefits of these efforts.

In spite of the importance of the questions, the literature on evaluating information sharing is quite thin. That lack, coupled with passionate arguments both for and against the value of such efforts, has produced a stunted policy debate that is insufficient to support reasoned and reasonable tradeoffs among these programs and other ways to pursue the security and other goals they are designed to advance. Part of the difficulties in this area appear to arise from the range of different initiatives that have been grouped under the general term *information sharing*, and this report has sought to distinguish them in reasonable and useful ways. With a clearer framing of the evaluable goals the programs are pursuing—transmission of alert and warning, sharing of data, dissemination of knowledge, and sharing of expertise—data on organizational outcomes can be linked to different ways of assessing the "dosage" of exposure to the information sharing at different levels. A focus on outcome measures is probably even more important here than in many other areas, since process or intermediate measures could provide a misleading picture of the actual effects of an initiative. While getting to outcomes is most straightforward when evaluation is built into the implementation of a new information sharing effort, new analytic techniques that enable matching of individual users and comparison of outcomes at a very disaggregated level appear particularly promising for assessing initiatives that are already in place.

Though clearly a difficult problem, since information shared through the myriad of activities and systems designed to improve intelligence, policing, and security performance is used for many different purposes, systematic approaches like the "but-for" analyses explored here and structures like that shown in Figure 2 that tie the sharing to the outcomes it is designed to achieve provide paths forward. In a world of finite resources at all levels of government, making these analytic investments now is important if future decisions about the preservation, maintenance, or expansion of these systems is to be based on objective data instead of assumptions and anecdotal evidence of their effects and value.

## Notes

[1] The response rate for the two-wave survey was relatively low, between 10 and 15 percent, potentially making even this significant count of information sharing systems an underestimate.

[2] Based on survey response rates varying between 48 and 76 percent, depending on respondent (police chief or analyst) and department size.

[3] One element of this literature is the willingness of organizations to share information and the organizational incentives that shape that willingness; although they are an important piece of the puzzle and a variable that can shape the value of a sharing effort, organizational-behavior issues are not the focus of this report.

[4] Contemporaneous with this writing, significant public disclosures were made regarding the collection of information domestically as part of federal-government counterterrorism and law enforcement efforts. Those revelations have stimulated debate regarding civil liberties. While those concerns are not a central focus of this report, it is relevant to keep in mind that civil-liberties concerns involve both the *collection* and the *sharing* of data, since both affect personal privacy and potentially impact individuals in different, if related, ways.

[5] In response to the 2012 Senate staff report, a number of law enforcement organizations questioned the findings and cited reporting by fusion centers of suspicious activity and reports from fusion centers to the Terrorist Screening Center as a source of resulting FBI JTTF investigations ("IACP Issues Joint Statement," 2012). In addition, at the federal level, the 2012 ISE Annual Report indicated that federal agencies surveyed by the Program Manager—Information Sharing Environment (PM-ISE) report that they use material produced by fusion centers to at least some degree (p. A-5).

[6] The critical Senate report on the fusion center program identified problems in DHS's ability to determine how much it had spent on that program (Permanent Subcommittee on Investigations, 2012, pp. 62–64).

[7] Information sharing can contribute to policy areas outside of security, e.g., in regulation or the management of common resources. These other policy areas are beyond the scope of this study.

[8] Weiss (1997) discusses interagency information sharing in policing related to innovation—i.e., identifying common solutions to problems or lessons learned about new methods—as being highly person-to-person, driven by "calling around" to other departments. One strength of this method of information sharing is the match in the backgrounds and perspectives of the seeker and receiver of the information, which increases the chances that what is shared will be well matched to the need.

[9] For example, in intelligence, one of the added values provided by analysts is the filtering of data that are important and valuable from data that might be interesting but are less critical. An extreme example of this is the preparation of the President's Daily Brief, in which an entire process and staff winnow the intelligence data and products of the day down to those the President most needs to hear. Insufficient winnowing would undermine the goal the process is trying to achieve, i.e., queuing up the most critical information for decision or action.

[10] These systems focus on the exchange of information that is captured in documents, operating procedures, and other explicit knowledge. In addition to examples like after-action reports, some products produced by the FBI for state and local agencies have been described this way: "Intelligence bulletins, issued weekly, are intended to share information with state and local law enforcement agencies on an unclassified, law-enforcement-sensitive basis. The Bulletins are not alerts that give specific guidance to law enforcement agencies on preventing a terrorist act, but rather *appear to be an effort to educate and raise general awareness about terrorism issues*" (Department of Justice, 2003, p. ix, emphasis added).

[11] Sharing of expertise may be a necessity to take full advantage of shared data, since the knowledge and skills needed to understand and apply the data may not all be resident in all receiving agencies. As a result, expertise sharing may be a path to gain access to the needed capabilities without requiring independent investments to build them in every agency.

[12] A discussion of the functions and measurement of the value of the FBI's task forces is illustrative in this respect:

> Traditionally, the FBI, like any law enforcement agency, measures performance with "hard" numbers, such as cases, arrests, and prosecutions. For counterterrorism efforts, the FBI officials and JTTF members we interviewed told us that these metrics are considered less useful and sometimes not valid because a case may never result in an arrest or a prosecution but instead may produce important intelligence or information that prevents a terrorist act. The quality of information generated by a source also may be more important in assessing task forces' success rather than the number of sources. Additionally, a terrorism investigation may continue for a much longer period than a traditional criminal investigation and will not demonstrate immediate measurable results. ATAC Coordinators and members told us that the ATACs are for the most part responsible for activities such as training, information sharing, and communication that may be better measured through feedback from their participants. The managers and members of the NJTTF and FTTTF told us that their task forces are primarily support organizations that may be better measured by the customers served and their assessments of timeliness and quality of the customer support provided. (Department of Justice, 2003)

[13] These steps relate to different portions of the traditional intelligence cycle, including collection, processing/collation, and dissemination (*see* Department of Justice, 2003).

[14] For example, see March (1994, pp. 80–82) discussing organizational processes of applying decision rules and evaluating their outcomes in light of new data; the three-part cycle described in Daft and Weick (1984) of data collection, interpretation, and action; or Boyd's well-known OODA loop (observe, orient, decide, and act) summarized in Partnoy (2012).

[15] Although, as one reviewer of this report appropriately noted, one benefit of sharing data is the reduction of the need for redundant investments in data collection in multiple agencies. The efficiency produced could be a significant offset for the costs of the sharing efforts, although assessing how it tips the cost-benefit balance for a sharing activity requires a way to assess how many other agencies would build their own standalone collection efforts. Assuming none of them would do so is probably as unrealistic as assuming that all would, but where on the spectrum reality would fall in the absence of the sharing effort is difficult to assess.

[16] Note that the focus here is on all *available* data—not *all* data or even all *necessary* data—since the problem at hand is the evaluation of sharing, not of intelligence or analytic efforts in general. Whether the actions taken at the end of the cycle depend on whether the "answer" reached through the other stages is correct depends on whether enough (and good enough) data were available in the first place. But the probability that the data available are *sufficient* to reach the right decision (versus the probability that all the relevant data available could be used as the decision is made) is driven by collection, and it would be inappropriate to penalize a sharing effort for not sharing data that it did not have in the first place.

[17] These distinctions among different steps are not simply an academic exercise. Depending on the problems that are affecting the performance of the system, interventions that affect one part may not have the desired effect on outcomes. Jones makes an argument that this is the case regarding intelligence sharing after 9/11, where the central focus was on data sharing, which would not address problems in recognizing and understanding relevant data (Jones, 2007).

[18] In principle, human-involved systems could be better positioned to be better filters, assuming they have the skills and authorities to do so. Technological systems can filter very efficiently, but doing so effectively can be difficult to implement (exemplified by both the strengths and weaknesses of most text search engines). Filtering creates interaction between the first step and the second. Sharing everything with no filter maximizes the chance that data will be collocated but increases the chance that it will not be noticed among the noise. Filtering more increases the chance that what is passed will be noticed but creates an increasing probability that important data will be filtered out as the "thickness" of the filter increases.

[19] Taking action may not require going outside a single organization, at which point the effectiveness of interagency information sharing is not a factor affecting success.

[20] As discussed elsewhere in this report, whether information being shared is irrelevant or of poor quality is a central element in the policy debate surrounding current efforts. It is important that generalizations about "useless data" be examined closely, and rather than being black and white, the issue involves varied shades of grey. Data or analytical products that are factually wrong are demonstrably useless and harmful, whatever the context. And data may be correct but unimportant. However, *unimportant* is less than a black-or-white designation. Data that are unimportant for current problems may be relevant and important in the future, though their inclusion might contribute to noise that makes it more difficult to find and use currently critical data.

[21] Politics shapes the choices organizations make about these tradeoffs. Even if reasonable tradeoffs are made about what to share and what not to in the interest of producing the best net performance of all steps of the cycle, if an event occurs and it can be shown that relevant, unshared data existed (even if the relevance is clear only in hindsight), the political price can be considerable.

[22] See Rossi, Lipsey, and Freeman, 2004, for a review.

[23] A summary of commonly used metrics is available in Bureau of Justice Assistance, undated(b).

[24] In both the academic and the policy literature, evaluations are reported, but most do not assess outcomes: In a Bureau of Justice Assistance review of past efforts, most are characterized as "either . . . usability evaluations or case studies" and therefore focus more on process or on the details of individual systems than on comprehensive assessment of output and outcomes (BJA, undated(c)).

[25] Whether arrests are viewed as an output or outcome measure varies, with clearance of past crimes more often treated as an outcome, although both are generally tied to the broader outcome of crime reduction through deterrence of future criminal behavior by increasing the certainty of punishment.

[26] The Senate report, in critiquing the meaning of the success stories provided as evidence for the value of fusion centers, raised a number of issues including the "counterfactual problem"—whether the information sharing being attributed to the centers would have occurred even if they were not present—as well as identifying cases where the contribution of centers appeared to have been counterproductive.

[27] Additional examples of evaluations focused on multijurisdictional task forces are available at Bureau of Justice Assistance, undated(d).

[28] "A lot of [the reporting] was predominantly useless information," according to a former Senior Reports Officer, who worked in the Reporting Branch from 2006 to 2010. "You had a lot of data clogging the system with no value." Overall, he estimated that 85 percent of the reports coming out of the Reporting Branch were "not beneficial" to any entity, from federal intelligence agencies to state and local fusion centers (Permanent Subcommittee on Investigations, 2012, p. 27).

[29] In describing the Interagency Threat Assessment and Coordination Group's activities, a group "comprised of representatives of State, local and tribal homeland security, law enforcement, fire, and health activities and Federal intelligence analysts assigned to the [NCTC]" (p. 1) described their goal as "to better inform [State, Local, Tribal, and private sector (SLTP)] partners on genuine terrorism threats, while diminishing the possibility of SLTP partners reacting improperly to reporting of low, questionable, or no credibility, during periods of heightened threat." (PM-ISE, 2010, pp. 9–10) This succinctly makes the data-quality argument for filtering, the companion rationale to reducing the probability of information overload and the probability that important data points will be lost in a sea of other data.

[30] See, for example, the discussion in Marrin, 2012, and the essay entitled "Why Can't Intelligence Products Get Rated Like Books on Amazon?" (Dinh, 2012).

[31] There is also the asymmetry that *negative* user evaluations can be more definitive than positive ones: If users do not like a system and do not perceive it as useful, their use of it will likely fall, increasing the likelihood of poor outcomes.

[32] See Center for Society, Law and Justice (2008) for a useful summary that is framed for information systems in general but is directly applicable to information sharing systems and activities.

[33] For example, Center for Society, Law and Justice (2008, p. 19) makes the point that data need to be recorded in a way that facilitates evaluation efforts. If evaluation is not planned for, ephemeral data may never be captured, making rigorous evaluation at a later date impossible.

[34] This issue was central in the Senate report that was critical of DHS's fusion center program: "In four success stories that DHS identified, the Subcommittee investigation was unable to confirm that the fusion centers' contributions were as significant as DHS portrayed them; were unique to the intelligence and analytical work expected of fusion centers; or would not have occurred absent a fusion center" (Permanent Subcommittee on Investigations, 2012, p. 83).

[35] In some areas, such cross-jurisdictional arrests are quite important. For example, in an examination of the Citizen and Law Enforcement Analysis and Reporting (CLEAR) program in Chicago, it was noted that "in Cook County, Illinois – 25% of some suburbs' arrests are Chicago residents" (Center for Criminal Justice Technology, 2007 ).

[36] This same logic does not necessarily apply to information *collection* efforts. Even if information collected today is not being accessed routinely, this does not mean that future use of it will not provide value—however, that value would be weighed against both the tangible and intangible costs of its collection and storage.

[37] Given the mix of goals captured by information sharing, the idea of "value added" as a way of normalizing more-ambiguous measures of usage or traffic is potentially very attractive. The more unique a system and its content are, the easier it is to trace their use in success stories (and to substantiate their particular value in "but-for" analysis) and, therefore, the greater the information content of process measures such as usage—i.e., if the specific data can be obtained only there, and the application of those data in achieving outcomes can be shown, then the amount practitioners or others seek those data has more meaning than, for example, the amount they use one of several more-general resources whose link to outcomes is harder to substantiate.

[38] Lane Burgette of RAND is gratefully acknowledged for this insight.

## Bibliography


9/11 Commission—*See* National Commission on Terrorist Attacks Upon the United States.

Bean, Hamilton, "Exploring the Relationship Between Homeland Security Information Sharing & Local Emergency Preparedness," *Homeland Security Affairs*, Vol. V, No. 2, May 2009. As of February 11, 2014: http://www.hsaj.org/?article=5.2.5

Behrens, Timothy E. J., Mark W. Woolrich, Mark E. Walton, and Matthew F. S. Rushworth, "Learning the Value of Information in an Uncertain World," *Nature Neuroscience*, Vol. 10, No. 9, September 2007, pp. 1214–1221.

BJA—*See* Bureau of Justice Assistance.

Bureau of Justice Assistance, "Commonly Used Measures of Information Sharing/Integration Initiatives," Washington, D.C., undated (b). As of February 11, 2014: https://www.bja.gov/evaluation/program-information-sharing/isii5.htm

———, "Justice Information Sharing: A 2010–2012 Strategic Action Plan, Accomplishments and Status Report," Washington, D.C., November 2012.

———, "Planning to Evaluate an Information Sharing/Integration Initiative? What Are Some Challenges?" Washington, D.C., undated (a). As of February 11, 2014: https://www.bja.gov/evaluation/program-information-sharing/isii4.htm

———, "What Have We Learned from Evaluations of Information Sharing/Integration Initiatives?" Washington, D.C., undated (c). As of February 11, 2014: https://www.bja.gov/evaluation/program-information-sharing/isii2.htm

Bureau of Justice Assistance, Center for Program Evaluation and Performance Measurement, "Publications," Washington, D.C., undated (d). As of February 11, 2014: https://www.bja.gov/evaluation/program-law-enforcement/forces6.htm

Carter, David L., "Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies," Michigan State University, School of Criminal Justice, November 2004.

Carter, Jeremy, and Steven Chermak, "Evidence-Based Intelligence Practices: Examining the Role of Fusion Centers as a Critical Source of Information," in Cynthia Lum and Leslie W. Kennedy, eds., *Evidence-Based Counterterrorism Policy*, Chap. 4, New York: Springer, 2012, pp. 65–88.

Center for Criminal Justice Technology, "Implementing Regional Law Enforcement Information Sharing Systems: Practitioner Views and Results from the Comprehensive Regional Information Sharing Project (CRISP)," presentation at the 31st Annual International Association of Chiefs of Police Law Enforcement Information Management (LEIM) Section Training Conference and Exposition, May 23, 2007. As of February 11, 2014: http://www.theiacp.org/Portals/0/pdfs/LEIM/2007Presentations/CRISP_Study_Results.pdf

Center for Society, Law and Justice, Texas State University, *Performance Measurement for Justice Information System Projects*, Bureau of Justice Assistance, March 2008. As of February 9, 2014: https://www.bja.gov/publications/jis_perform_meas.pdf

Chen, Hsinchun, et al., "COPLINK Connect: Information and Knowledge Management for Law Enforcement," *Decision Support Systems*, Vol. 34, 2002, pp. 271–285.

Clemen, Robert T., and Robert L. Winkler, "Limits for the Precision and Value of Information from Dependent Sources," *Operations Research*, Vol. 33, No. 2, March/April 1985, pp. 427–442.

Conrad, Jon M., "Quasi-Option Value and the Expected Value of Information," *The Quarterly Journal of Economics*, Vol. 94, No. 4, June 1980, pp. 813–820.

Daft, Richard L., and Karl E. Weick, "Toward a Model of Organizations as Interpretation Systems," *The Academy of Management Review*, Vol. 9, No. 2, April 1984, pp. 284–295.

Darilek, Richard E., Walter L. Perry, Jerome Bracken, John Gordon IV, and Brian Nichiporuk, *Measures of Effectiveness for the Information Age Army*, Santa Monica, Calif.: RAND, MR-1155-A, 2001. As of February 11, 2014: http://www.rand.org/pubs/monograph_reports/MR1155.html

Davies, Heather J., and Martha R. Plotkin, *Protecting Your Community from Terrorism: The Strategies for Local Law Enforcement Series, Vol. 5: Partnerships to Improve Homeland Security*, Washington, D.C.: Office of Community Oriented Policing Services and Police Executive Research Forum, 2005.

Davis, James, "The Role of the Fusion Center in Counterterrorism Operations," *The Police Chief*, February 2013, pp. 20–26.

Davis, Lois M., Michael Pollard, Kevin Ward, Jeremy M. Wilson, Danielle M. Varda, Lydia Hansell, and Paul S. Steinberg, *Long-Term Effects of Law Enforcement's Post-9/11 Focus on Counterterrorism and Homeland Security*, Santa Monica, Calif.: RAND Corporation, MG-1031-NIJ, 2010. As of February 8, 2014: http://www.rand.org/pubs/monographs/MG1031.html

Department of Homeland Security, "2011 National Network of Fusion Centers: Final Report," Washington, D.C., May 2012.

———, "Fusion Center Activities," Washington, D.C., undated. As of February 11, 2014:
http://www.dhs.gov/fusion-center-success-stories

Department of Justice, *National Criminal Intelligence Sharing Plan*, Washington, D.C., October 2003.

Dethlefs, David R., "Information Sharing and Interoperability in Law Enforcement: An Investigation of Federal Criminal Justice Information Systems Use By State/Local Law Enforcement Organizations," master's thesis, Air Force Institute of Technology, Wright-Patterson AFB, Ohio, 2003.

Dinh, Thanh "Tino," "Why Can't Intelligence Products Get Rated Like Books on Amazon?" National Intelligence Writing Contest winner, Armed Forces Communications and Electronics Association, 2012. As of August 28, 2013:
http://www.afcea.org/mission/intel/Products.pdf

Felli, James C. and Gordon B. Hazen, "Sensitivity Analysis and the Expected Value of Perfect Information," *Medical Decision Making,* Vol. 18, No. 1, 1997, pp. 95–109.

Feltham, Gerald A., "The Value of Information," *The Accounting Review*, Vol. 43, No. 4 (Oct., 1968), pp. 684-696.

GAO—*See* Government Accountability Office.

Government Accountability Office, "Information Sharing: Additional Actions Could Help Ensure That Efforts to Share Terrorism-Related Suspicious Activity Reports Are Effective," Washington, D.C., GAO-13-233, March 2013a.

———, "Information Sharing: Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities," Washington, D.C., GAO-13-471, April 2013b.

———, "Information Sharing: Capabilities and Protect Privacy, but Could Better Measure Results," Washington, D.C., GAO-10-972, September 2010a.

———, "Information Sharing: Definition of the Results to Be Achieved in Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress," Washington, D.C., GAO-08-637T, July 2008.

———, "Information Sharing: DHS Could Better Define How It Plans to Meet Its State and Local Mission and Improve Performance Accountability," Washington, D.C., GAO-11-223, December 2010b.

———, "Information Sharing: DHS Has Demonstrated Leadership and Progress, but Additional Actions Could Help Sustain and Strengthen Efforts," Washington, D.C., GAO-12-809, September 2012.

———, "Information Sharing: Progress Made and Challenges Remaining in Sharing Terrorism-Related Information," Washington, D.C., GAO-12-144T, October 2011.

Hauck, Roslin V., "Should They Share or Not? An Investigation on the Use of Communication and Knowledge Sharing Technology in a Police Organization," dissertation, Tucson, Ariz.: University of Arizona, 2005.

Hawley, Kip, and Nathan Means, *Permanent Emergency: Inside the TSA and the Fight for the Future of American Security*, New York: Palgrave Macmillan, 2012.

Hayeslip, David W., and Malcolm L. Russell-Einhorn, *Evaluation of Multi-Jurisdictional Task Forces Project: Phase I Final Report*, Washington, D.C.: Abt Associates, 2002.

IACP—*See* International Association of Chiefs of Police.

"IACP Issues Joint Statement with Leadership Organizations Re: Fusion Center Report," Official Blog of the International Association of Chiefs of Police, October 4, 2012. As of February 7, 2014:
http://theiacpblog.org/2012/10/04/iacp-issues-joint-statement-with-leadership-organizations-re-fusion-center-report/

Information Sharing Environment, "Annual Report to the Congress," June 30, 2012.

———, "Law Enforcement Information Sharing," undated. As of February 11, 2014:
http://www.ise.gov/law-enforcement-information-sharing

International Association of Chiefs of Police, "National Summit on Intelligence: Gathering, Sharing, Analysis, and Use After 9-11: Measuring Success and Setting Goals for the Future," September 2008. As of February 11, 2014:
http://www.theiacp.org/portals/0/pdfs/IntelSummitReport.pdf

ISE—*See* Information Sharing Environment.

Jackson, Brian A. "Exploring Measures of Effectiveness for Domestic Intelligence: Addressing Questions of Capability and Acceptability," in Brian A. Jackson, ed., *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency*, Santa Monica, Calif.: RAND Corporation, MG-804-DHS, 2009b, pp. 179-204. As of February 11, 2014:
http://www.rand.org/pubs/monographs/MG804.html

———, "Exploring the Utility for Considering Cost-Effectiveness Analysis of Domestic Intelligence Policy Change," in Brian A. Jackson, ed., *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency*, Santa Monica, Calif.: RAND Corporation, MG-804-DHS, 2009b, pp. 205-238. As of February 11, 2014:
http://www.rand.org/pubs/monographs/MG804.html

Jackson, Brian A., Darcy Noricks, and Benjamin W. Goldsmith, "Current Domestic Intelligence Efforts in the United States," in Brian A. Jackson, ed., *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency*, Santa Monica, Calif., RAND Corporation, MG-804-DHS, 2009, pp. 49–78. As of February 11, 2014:
http://www.rand.org/pubs/monographs/MG804.html

Jones, Calvert. "Intelligence Reform: The Logic of Information Sharing," *Intelligence and National Security*, Vol. 22, No. 3, June 2007, pp. 384–401.

Kaiser, Frederick M., "Access to Classified Information: Seeking Security Clearances for State and Local Officials and Personnel," *Government Information Quarterly*, Vol. 20, No. 3, 2003, pp. 213–232.

Lamb, Christopher J., and Evan Munsing, "Secret Weapon: High-Value Target Teams as an Organizational Innovation," Strategic Perspectives 4, Washington, D.C.: Center for Strategic Research, National Defense University, 2011.

Lammers, Marre, and Wim Bernasco, "Are Mobile Offenders Less Likely to Be Caught? The Influence of the Geographical Dispersion of Serial Offenders' Crime Locations on Their Probability of Arrest," *European Journal of Criminology*, Vol. 10, No. 2, 2013, pp. 168–186.

Lester, Genevieve. "Societal Acceptability of Domestic Intelligence," in Brian A. Jackson, ed., *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency*, Santa Monica, Calif.: RAND Corporation, MG-804-DHS, 2009, pp. 79-104. As of February 11, 2014:
http://www.rand.org/pubs/monographs/MG804.html

Libicki, Martin C., and Shari Lawrence Pfleeger, *Collecting the Dots: Problem Formulation and Solution Elements*, Santa Monica, Calif.: RAND Corporation, OP-103-RC, 2004. As of February 11, 2014:
http://www.rand.org/pubs/occasional_papers/OP103.html

March, James G., *A Primer on Decision Making: How Decisions Happen*, New York: The Free Press, 1994.

Marrin, Stephen, "Evaluating the Quality of Intelligence Analysis: By What (Mis) Measure?" *Intelligence and National Security*, Vol. 27, No. 6, December 2012, pp. 896–912.

McCarthy, John. "Measures of the Value of Information," *Proceedings of the National Academy of Sciences*, Vol. 42, 1956, pp. 654–655.

McFeely, Richard A., "Information Sharing with Partners Span Many FBI Programs," testimony before the Senate Judiciary Committee, Wilmington, Del., June 20, 2011.

National Commission on Terrorist Attacks Upon the United States, *Final Report of the National Commission on Terrorist Attacks Upon the United States*, New York: W.W. Norton & Company, 2004.

National Consortium for Justice Information and Statistics, "Information Sharing Case Study: Los Angeles County, California," 2009. As of February 11, 2014:
http://www.search.org/files/pdf/LA_County_Case_Study.pdf

*National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*, October 2007. As of February 8, 2014:
http://www.ise.gov/sites/default/files/nsis.book.pdf

Noblis, Inc., *Comprehensive Regional Information Sharing Project, Volume 1: Metrics for the Evaluation of Law Enforcement Information Sharing Systems*, Noblis Technical Report MTR-2006-035, Falls Church, Va., January 2007.

Odabasi, Mehmet, "User Acceptance of North Central Texas Fusion Center System by Law Enforcement Officers," dissertation, Denton, Tex.: University of North Texas, 2010.

Office of the Inspector General, U.S. Department of Justice, *The Federal Bureau of Investigation's Efforts to Improve the Sharing of Intelligence and Other Information*, Audit Report 04-10, December 2003 (redacted and unclassified).

———, *The Department of Justice's Terrorism Task Forces*, I-2005-007, June 2005.

Olson, David E., et al., "New Approaches and Techniques for Examining and Evaluating Multi-Jurisdictional Drug Task Forces in Illinois," Chicago, Ill.: Loyola University, December 2002. As of February 11, 2014:
http://www.icjia.state.il.us/public/pdf/ResearchReports/NewApproaches.pdf

Partnoy, Frank, "Act Fast, but Not Necessarily First," Harvard Business Review Blog, July 13, 2012. As of February 11, 2014:
http://blogs.hbr.org/2012/07/act-fast-not-first

Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, United States Senate. *Federal Support for and Involvement In State and Local Fusion Centers*, Majority and Minority Staff Report, Washington, D.C., October 3, 2012.

Perry, Walter L., Robert W. Button, Jerome Bracken, Thomas Sullivan, and Jonathan Mitchell, *Measures of Effectiveness for the Information-Age Navy: The Effects of Network-Centric Operations on Combat Outcomes*, Santa Monica, Calif.: RAND Corporation, MR-1449-NAVY, 2002. As of February 11, 2014:
http://www.rand.org/pubs/monograph_reports/MR1449.html

Perry, Walter L., and James Moffat, *Information Sharing Among Military Headquarters: The Effects on Decisionmaking*, Santa Monica, Calif.: RAND Corporation, MG-226-UK, 2004. As of February 11, 2014:
http://www.rand.org/pubs/monographs/MG226.html

*Information* PM-ISE—*See* Program Manager—Information Sharing Environment.

Powner, David, A. "Information Technology: Homeland Security Information Network Needs to Be Better Coordinated with Key State and Local Initiatives," U.S. Government Accountability Office, GAO-07-822T, testimony before the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, Committee on Homeland Security, House of Representatives, May 10, 2007.

Program Manager—Information Sharing Environment, *2010 Report on the Interagency Threat Assessment and Coordination Group (ITACG)*, 2010. As of February 11, 2014: https://www.ise.gov/sites/default/files/2010_ITACG_Report_Final_30Nov10.pdf

Rhodes, William, Meg Chapman, Michael Shively, Christina Dyous, Dana Hunt, and Kristin Wheeler, *Evaluation of the Multijurisdictional Task Forces (MJTFs), Phase II, Project Summary*, Washington, D.C.: Abt Associates, 2009a.

Rhodes, William, Christina Dyous, Meg Chapman, Michael Shively, Dana Hunt, and Kristin Wheeler, *Evaluation of the Multijurisdictional Task Forces (MJTFs), Phase II, MJTF Performance Monitoring Guide,* Washington, D.C.: Abt Associates, 2009b.

Rossi, Peter H., Mark W. Lipsey, and Howard E. Freeman, *Evaluation: A Systematic Approach*, 7th ed., Thousand Oaks, Calif.: SAGE, 2004.

Rojek, Jeff, Robert J. Kaminski, Hayden Smith, and Mikaela Cooney, *2010 South Carolina Law Enforcement Census: Local Law Enforcement Use and Evaluation of the South Carolina Intelligence and Information Center*, Columbia, S.C.: University of South Carolina, Department of Criminology and Criminal Justice, October 2010.

Russell-Einhorn, Malcolm, Shawn Ward, and Amy Seeherman, *Federal-Local Law Enforcement Collaboration in Investigating and Prosecuting Urban Crime, 1982–1999: Drugs, Weapons, and Gangs*, Washington, D.C.: Abt Associates, 2004.

Sandler, Todd, "Law Enforcement Information Sharing and the Implications for Local Government," Digital Communities, 2010. As of February 11, 2014: http://www.digitalcommunities.com/library/papers/Law-Enforcement-Information-Sharing-and-the.html

Scott, Ernest D.. *Factors Influencing User-Level Success in Police Information Sharing: An Examination of Florida's FINDER System*, dissertation, Orlando, Fla.: University of Central Florida, 2006.

Skogan, Wesley G., and Susan M. Hartnett, "The Diffusion of Information Technology in Policing," *Police Practice and Research*, Vol. 6, No. 5, December 2005, pp. 401–417.

Skogan, Wesley G., et al., "Policing Smarter Through IT: Learning from Chicago's Citizen and Law Enforcement Analysis and Reporting (CLEAR) System," U.S. Department of Justice, Office of Community Oriented Policing Services, Washington, D.C., December 2003.

Wagner, Lisa Walbolt "Information Sharing Systems: A Survey of Law Enforcement," Justice Research and Statistics Association, July 2006.

Wagner, Lisa Walbolt "Use of Data in Police Departments: A Survey of Police Chiefs and Data Analysts," Washington, D.C.: Justice Research and Statistics Association, May 2005.

Weiss, Alexander, "The Communication of Innovation in American Policing," *Policing: An International Journal*, Vol. 20, No. 2, 1997, pp. 292–310.

Zaworski, Martin J., "An Assessment of an Information Sharing Technology (ARJIS): Examining its Potential Contribution to Improved Performance Through the Eyes of Street Level Officers," Washington, D.C.: National Criminal Justice Research Service, NCJRS 210487, July 2005.

## About This Report

This research was conducted within the RAND Homeland Security and Defense Center, a joint center of RAND Justice, Infrastructure, and Environment, and the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

The work builds on past RAND work on criminal justice and domestic security, including

- Brian A. Jackson et al., *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency*, Santa Monica, Calif.: RAND Corporation, MG-804-DHS, 2009.
- Lois M. Davis et al., *Long-Term Effects of Law Enforcement's Post-9/11 Focus on Counterterrorism and Homeland Security*, Santa Monica, Calif.: RAND Corporation, MG-1031-NIJ, 2010.
- Walter L. Perry and James Moffat, *Information Sharing Among Military Headquarters: The Effects on Decisionmaking*, Santa Monica, Calif.: RAND Corporation, MG-226-UK, 2004.

The input of Lane Burgette of RAND on assessing self-selection biases among user choices to use information sharing systems is gratefully acknowledged. I would also like to acknowledge the contributions of Jeremy Wilson of Michigan State University, Andrew Liepman of RAND, Rob Flowe of the Department of Defense, and William Ford of the National Institute of Justice for their thoughtful reviews of the manuscript.

## The RAND Homeland Security and Defense Center

The RAND Homeland Security and Defense Center (HSDC) conducts analysis to prepare and protect communities and critical infrastructure from natural disasters and terrorism. Center projects examine a wide range of risk-management problems, including coastal and border security, emergency preparedness and response, defense support to civil authorities, transportation security, domestic intelligence, and technology acquisition. Center clients include the U.S. Department of Homeland Security, the U.S. Department of Defense, the U.S. Department of Justice, and other organizations charged with security and disaster preparedness, response, and recovery.

HSDC is a joint center of two research divisions: RAND Justice, Infrastructure, and Environment and the RAND National Security Research Division. RAND Justice, Infrastructure, and Environment is dedicated to improving policy and decisionmaking in a wide range of policy domains, including civil and criminal justice, infrastructure protection and homeland security, transportation and energy policy, and environmental and natural resource policy. The RAND National Security Research Division conducts research and analysis for all national security sponsors other than the U.S. Air Force and the Army. The division includes the National Defense Research Institute, a federally funded research and development center whose sponsors include the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the defense agencies, and the U.S. Department of the Navy. The National Security Research Division also conducts research for the U.S. intelligence community and the ministries of defense of U.S. allies and partners. For more information about the Homeland Security and Defense Center, see http://www.rand.org/hsdc or contact the director at hsdc@rand.org.

© Copyright 2014 RAND Corporation
ISBN 978-0-8330-386-9

**www.rand.org**


The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND focuses on the issues that matter most, such as health, education, national security, international affairs, law and business, the environment, and more. As a nonpartisan organization, RAND operates independent of political and commercial pressures. We serve the public interest by helping lawmakers reach informed decisions on the nation's pressing challenges. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

RR-380-OSD